FACULTAD DE POSTGRADOS

MAESTRÍA EN DERECHO DIGITAL E INNOVACIÓN CON MENCIÓN EN ECONOMÍA, CONFIANZA Y TRANSFORMACIÓN DIGITAL

TÍTULO DE LA INVESTIGACIÓN

Análisis técnico-jurídico de la obligación que tiene la Dirección Nacional de Tecnologías de la Información y Comunicación de la Policía Nacional del Ecuador de notificar la vulneración de seguridad de datos personales, año 2022

Profesor

Dra. Lorena Naranjo

Dr. Patricio Andino Sosa

Autores

Jorge Hugo Carvajal Gaibor

Diana Guadalupe Pozo Escobar

2022-2023

Tabla de contenido

1. RESUMEN

Uno de los problemas internacionales que ha afectado la seguridad de los Estados son los ciberataques, por lo tanto, para la seguridad de un Estado se necesita la implementación de normativa, protocolos y guías que ayuden a la prevención y solución de las posibles amenazas, riesgos y vulneraciones. La Policía Nacional del Ecuador es una de las instituciones estatales que brinda seguridad al Estado pues su misión fundamental, estipulada en la Constitución del Ecuador (artículo 163), es la de otorgar seguridad ciudadana y orden público; sin embargo, esta institución no está exenta de ciberataques que pueden recaer, por ejemplo, en su Dirección Nacional de Tecnologías de la Información y Comunicación, vulnerando la seguridad de los datos personales de los servidores policiales, otorgando a bandas delictivas la posibilidad de conocer el estado de los mismos y de su trabajo poniendo en riesgo el cumplimiento de su misión, pero además poniendo en riesgo sus derechos y libertades fundamentales; por tanto, al ocurrir estas vulneraciones la Ley Orgánica de Protección de Datos Personales no puede hacerse cargo ya que no se encuentra dentro de su ámbito de aplicación haciendo necesaria la creación de protocolos o guías que ayuden a salvaguardar estos datos personales y a conocer cómo se debe actuar en caso de que existiera un ciberataque, en beneficio del Estado y de los derechos y libertades fundamentales de los servidores policiales.

Palabras clave: Seguridad ciudadana, notificación, datos personales, servidores policiales, ámbito de aplicación, ciberataque.

2. ABSTRACT

One of the international problems that has affected the security of States are cyber attacks, therefore, for the security of a State, the implementation of regulations, protocols and guides is

needed to help prevent and solve possible threats, risks and violations. The National Police of Ecuador is one of the state institutions that provides security to the State since its fundamental mission, stipulated in the Constitution of Ecuador (article 163), is to grant citizen security and public order; However, this institution is not exempt from cyberattacks that may fall, for example, on its National Directorate of Information and Communication Technologies, violating the security of the personal data of police servers, giving criminal gangs the possibility of knowing the their status and their work jeopardizing the fulfillment of their mission, but also jeopardizing their rights and fundamental freedoms; therefore, when these violations occur, the Organic Law on the Protection of Personal Data cannot take charge since it is not within its scope of application, making it necessary to create protocols or guides that help safeguard this personal data and to know how it should be done. act in the event of a cyberattack, for the benefit of the State and the fundamental rights and freedoms of police officers.

Keywords: Citizen security, notification, personal data, police officers, scope of application, cyberattack

3. INTRODUCCIÓN

La innovación diaria de la tecnología obliga a que el Estado se vea inmerso en procesos de capacitación continua y, que, a través del conocimiento, Instituciones Públicas y Administrativas, como la de la Policial Nacional, puedan ser asistidas de manera óptima, oportuna y acorde a las exigencias actuales. La inseguridad dentro de los sistemas digitales a nivel nacional se intensifica cada vez más por lo que es necesario asesorar y promover la innovación y desarrollo tecnológico dentro de las distintias instituciones a nivel nacional de control social con respecto a las Tecnologías de la Información y Comunicaciones (TIC's) pues los datos que manejan son de carácter sensible. El presente proyecto busca asesorar a las dependencias policiales en la planeación, notificación, diseño, promoción, desarrollo, implementación y administración de las Tecnologías de la Información y la Comunicación, para el mejoramiento continuo del servicio que se brinda a la ciudadanía.

3.1. Contexto del entorno interno de la organización

La Dirección Nacional de Tecnologías de la Información y Comunicación de la Policía Nacional, fue creada mediante Resolución del Consejo de Generales No. 00-336-CGPN, publicada mediante Orden General No. 191, de fecha 03 de Octubre del 2000, con la finalidad de liderar la presentación de los servicios de comunicaciones e informática, a través de una constante preparación del elemento humano y la utilización de la tecnología adecuada que garantice la eficiencia y eficacia en su empleo, en beneficio institucional y de la comunidad.

Mediante Acuerdo Ministerial 0080, suscrito por la señora ministra del Interior con fecha 08 de marzo del 2019 se acuerda expedir el Estatuto Orgánico de Gestión Organizacional por Procesos de la Policía Nacional en el cual se establece la nueva denominación de la Dirección

Nacional de Comunicaciones en el Art. 40 siendo la Dirección Nacional de Tecnologías de la Información y Comunicación de la Policía Nacional.

3.2. Contexto del entorno externo de la Dirección Nacional de Tecnología de la Información y Comunicación

Con el aparecimiento, avance e innovación de las tecnologías en el mundo se crean también, a lo largo de los años, vulneraciones informáticas que dan origen a debates sobre la regulación del espacio cibernético; varios países alrededor del mundo han implementado normativas que regulan las nuevas tecnologías, así como los ataques que puede llegar a sufrir la seguridad informática y los protocolos que ayudan a la prevención y solución de las posibles amenazas, riesgos y vulneraciones; la normativa ISO 27001 es un claro ejemplo de lo expuesto.

Ecuador, es uno de los países que ha tenido la necesidad de incluirse dentro de planes y políticas de seguridad al ciberespacio pues busca salvaguardar la información de sus organismos, de sus servidores públicos y de la ciudadanía en general con el desarrollo de su seguridad informática que propicia estrategias que faciliten la "detección, prevención, mitigación y eliminación de ataques informáticos, los mismos que son considerados como principales amenazas" (Polo, 2016, p. 1). Para esto, Ecuador ha implementado el uso de las normas ISO 27000, el acuerdo ministerial EGSI (Esquema Gubernamental de Seguridad de la Información) y la reciente Ley Orgánica de Protección de Datos, además de las consideraciones de los más altos estándares internacionales en protección de datos como las guías de la Agencia Española de Protección de Datos.

Ecuador tiene una pequeña economía "dolarizada", bastante abierta y muy dependiente de los ingresos del petróleo que representan entre el 14 y el 20% del PIB más de la mitad de los ingresos procedentes de las exportaciones y entre el 20 y el 30% de los ingresos públicos. (WTI,

2012). Los tres primeros meses del 2022 y el año 2021 según el Banco Central del Ecuador el crecimiento de la economía fue de 0,4%. (BCE, 2022). Sin embargo, esto no es suficiente pues, Ecuador aún no despierta en la utilidad que tiene la tecnología por los pocos recursos que posee y por la poca inversión que tiene hacia la misma y esto se evidencia en la proforma presupuestaria 2022 que coloca 592,896.00 dólares al programa de Fomento de la Industria y Servicios de Tecnologías de la Información Y Comunicación.

3.3. Problema de investigación

Con la aprobación de la Ley Orgánica de Datos Personales publicada el 26 de Mayo de 2021, las instituciones públicas y privadas al ser responsables del tratamiento de datos están obligados a proteger los datos personales de todos los ciudadanos, por lo que para la Dirección Nacional de Tecnologías de la Información y Comunicación de la Policía Nacional del Ecuador, en aras de garantizar y estar apegado a la presente Ley, surge la necesidad de investigar la obligación que tiene esta institución pública para notificar vulneraciones a la seguridad de datos personales y cuál sería su protocolo basándose en toda la normativa existente.

3.4. Antecedentes teóricos del problema

Con el paso del tiempo y con el avance que ha tenido la tecnología, también han avanzado los delitos tecnológicos, tal es el caso de los ciberataques, mismos que han ocasionado problemas a las infraestructuras públicas de varios países. Un claro ejemplo de estos ciberataques fue el de WannaCry en 2017 que infectó a computadoras con un programa que encriptaba archivos y que pedía dinero para poder recuperarlos, este ataque que se dio en más de 140 países afectó a más de 230 mil ordenadores (Jaimovich, 2018) y se vieron comprometidos varios sectores de estos países como la salud, la telefonía, las empresas de transporte, etc. Otro de los ataques que se dieron en ese mismo año fue el de NotPetya, que infectó más de 16 mil máquinas con un costo de más de

mil millones de dólares. (Johnson, 2018). Este ciberataque afectó al funcionamiento normal de ciertos países, en especial el de Ucrania en donde oficinas gubernamentales, centros nucleares y demás instituciones del estado se fueron afectados. (Carrera, 2019). Ecuador también sufrió el ciberataque de WannaCry y fue el tercer país más afectado de Latinoamérica (Ecuavisa, 2017). Es por este tipo de ataques que se espera que los países implementen sistemas de seguridad y con ello puedan prepararse, prevenir y enfrentar cualquier ataque cibernético guiándose en normativas internacionales y creando protocolos para la actuación interna de cada país.

Para el Ecuador, el crecimiento diario de la tecnología y la existencia de un sin número de hardware y software, crean la necesidad de generar un sistema de seguridad de la información y obligan a que servidores públicos y civiles deban encontrarse inmersos en procesos de capacitación continua. Así, es necesario que, a través del conocimiento, las Institución Públicas y Administrativas puedan ser asistidas de manera óptima, oportuna y acorde a las exigencias actuales, pues la inseguridad dentro de los sistemas digitales a nivel nacional se intensifica cada vez más, por lo cual es esencial asesorar y promover la innovación y desarrollo tecnológico dentro de las distintas instituciones a nivel nacional con respecto a las Tecnologías de la Información y Comunicaciones (TIC's).

Con la aprobación de la Ley Orgánica de Datos Personales, las instituciones públicas y privadas, al ser responsables del tratamiento de datos, están obligados a protegerlos. Una de las instituciones públicas que trabaja con estos datos personales es, efectivamente, la Policía Nacional del Ecuador pues su Dirección Nacional de Tecnologías de la Información y Comunicación es la responsable de la protección de datos de los servidores policiales; sin embargo, surge la problemática de conocer la obligación que tiene esta institución acerca de notificar la vulneración de la seguridad de datos personales de estos servidores pues en ciertos casos podría generar un riesgo a ciertos derechos fundamentales o libertades individuales.

4. REVISIÓN DE LITERATURA

4.1. Marco conceptual

4.1.1. Área Técnica

- **Seguridad de la Información.**

  González (2011) menciona que es una "disciplina que se encargaría de las implementaciones técnicas de la protección de la información, despliegue de tecnologías antivirus, firewalls, detección de intrusos, detección de anomalías, correlación de eventos, atención de incidentes, entre otros, que establecen la forma de actuar y asegurar las situaciones de fallas parciales o totales, cuando la información es el activo que se encuentra en riesgo".

- **Datos Personales**

  Según Miguel Julio (2015) “Un dato personal es cualquier información concerniente a una persona”, por otro lado, la Ley Orgánica de Protección de Datos Personales (2021) menciona que un dato personal es un “Dato que identifica o hace identificable a una persona natural, directa o indirectamente”.

- **Datos Sensibles**

  “Datos relativos a: etnia, identidad de género, identidad cultural, religión, ideología, filiación política, pasado judicial, condición migratoria, orientación sexual, salud, datos biométricos, datos genéticos y aquellos cuyo tratamiento indebido pueda dar origen a discriminación, atenten o puedan atentar contra los derechos y libertades fundamentales.” (Ley Orgánica de Protección de Datos Personales, 2021)

- **Protección de datos**

Según Rallo Lombarte (2019) se trata de un derecho fundamental que "persigue garantizar a la persona el poder de control sobre sus datos personales, sobre su uso y destino, con el propósito de impedir su tráfico ilícito y lesivo para la dignidad y derecho del afectado"

- **Notificación**

  Según la Guía para la Notificación de Brechas de Datos Personales de la Agencia Española de Protección de Datos (2021), la notificación es "una evidencia de la diligencia de la organización a la hora de ejecutar eficazmente la obligación de responsabilidad proactiva requerida por el Reglamento General de Protección de Datos". Establece que su finalidad es "la protección efectiva de los derechos fundamentales y libertades de las personas físicas afectadas por la brecha".

4.1.2. Área Jurídica

- **Bien jurídico protegido**

  El bien jurídico son aquellos bienes intrínsecos de cada una de las personas que deben ser protegidos por el Estado; y se considera a aquel elemento que determina el injusto de cada delito. Los bienes jurídicos pueden ser individuales como colectivos, en el presente caso nos centraremos en los individuales que vienen a ser aquellos que sirven a una persona o son de su titularidad.

- **Derecho fundamental**

  Según la Declaración Universal de los Derechos Humanos (1948) son aquellos derechos reconocidos por la constitución o la ley; así mismo, la RAE menciona que son "derechos declarados por la Constitución que gozan del máximo nivel de protección". Estos derechos son alienables, inviolables e irrenunciables y se diferencian de los derechos humanos por la territorialidad ya que los derechos fundamentales son los que aparecen en la Constitución

de cada país mientras que los derechos humanos son de carácter universal. (Oxfam Intermón, 2020)

- **Libertad individual**

  Para Sosa S. (2018) la libertad viene a ser "la ausencia de la interferencia", es decir, el actuar sin restricciones sino con autonomía, y, por otro lado, esta libertad también implica el desarrollo de la libre personalidad.

  Además, la libertad individual según González P. (2017) es catalogada como un bien jurídico que se expone al individuo en su vida cotidiana como un sentido natural de libertad.

  - **¿Qué es vida?**

    La vida es un derecho humano y fundamental establecido tanto en la Declaración Universal de los Derechos Humanos como en las distintas Constituciones; Cabanellas (2006) menciona que se trata de la manifestación, la actividad y el funcionamiento orgánico del ser, y también es el tiempo que transcurre desde que el ser nace hasta que muere.

  - **¿Qué es libertad?**

    El Diccionario Elemental de Guillermo Cabanellas (2006), menciona que Justiniano define a la libertad como aquella facultad natural en la que cada uno hace lo que quiere excepto aquello que le impide la fuerza o el Derecho.

    La Constitución menciona en su artículo 66 que la libertad es un derecho que garantiza y reconoce más derechos como el de la propia integridad personal que comprende la integridad física, psíquica, moral y sexual.

  - **¿Qué es integridad personal?**

José Miguel Guzmán menciona que la integridad personal es un derecho humano fundamental que busca el respeto a la vida y el desarrollo sano de la misma. Busca conservar la integridad física, psíquica y moral del ser humano.

La integridad física se refiere a cuidar las partes del cuerpo y la salud de la persona, la integridad psíquica cuida las habilidades motrices, psicológicas, intelectuales y emocionales; y la integridad moral que se refiere al derecho de desarrollar la vida de acuerdo a las convicciones que cada uno tiene.

El artículo 45 de la Constitución menciona el derecho a la integridad física y psíquica.

- **Seguridad Ciudadana**

  La seguridad ciudadana puede ser definida como aquella política del Estado necesaria para que se pueda fortalecer o modernizar aquellos mecanismos que sirven para garantizar los Derechos Humanos, especialmente el derecho a vivir libre de violencia, la protección de víctimas y la ciudadanía en general, y el mejoramiento de la calidad de vida de todos quienes habitan en el Ecuador. (Ministerio del Interior del Ecuador, 2019). Esta seguridad ciudadana se logra con la acción integrada desarrollada por parte del Estado en colaboración con la ciudadanía y organizaciones de protección y bien público. (Benavides, Benavides, Santillán; 2021)

- **Estándar Internacional**

  Un estándar internacional se refiere a una medida normativa establecida que se usa para juzgar la conducta que tiene un Estado respecto de los derechos humanos. (Condé, 1999)

4.2. Marco Teórico

CAPÍTULO 1

1.1. Protección Interna y Mantenimiento Del Orden Público

La Policía Nacional del Ecuador, según el artículo 158 de la Constitución, es una institución que protege los derechos, las libertades y las garantías que tienen los ciudadanos en el Estado; su función y responsabilidad principal es la "protección interna y el mantenimiento del orden público"; debe cumplir con su misión según el principio de obediencia establecido en la Constitución (artículo 159) siempre sujeto a la soberanía y a la norma suprema.

Que la Policía Nacional del Ecuador tenga como finalidad principal la protección interna y mantenimiento del orden público se da porque ésta es una institución que fue creada con el fin de proteger a su ciudadanía, de proteger sus derechos, libertades y garantías y esto se logra con la capacitación de sus servidores policiales, con el mantenimiento necesario del orden público para obtener el cumplimiento constante de su deber y la protección de todo aquel que forma parte del Ecuador; todo esto para que el Estado encuentre armonía y sus ciudadanos se encuentren protegidos de cualquier amenaza que se presente ya sea que se hable de una desestabilización al Estado o se hable de una violación o vulneración de los derechos, libertades y garantías de los ciudadanos

1.1.1. Misión de La Policía Nacional

La misión es el propósito de una institución; es la razón fundamental de su existencia. Es decir que la misión indica los límites de las actividades de una institución. (Dirección Nacional de Planificación y Gestión Estratégica, 2021)

La Policía Nacional del Ecuador configurada como una institución estatal tiene como misión fundamental, según la Constitución de la república (2008), el "atender la seguridad ciudadana y el orden público, y proteger el libre ejercicio de los derechos y la seguridad de la ciudadanía" (artículo 163); todo esto lo hace con una formación basada principalmente en los derechos humanos.

Así mismo, el Código Orgánico de las Entidades de Seguridad Ciudadana y Orden Público es más específico y detallado al mencionar la misión de la Policía Nacional del Ecuador y manifiesta que esta consiste en "la protección interna, la seguridad ciudadana, el mantenimiento del orden público que está en su competencia, el apoyo a la administración de justicia y la seguridad de la ciudadanía"; esta misión la cumple con subsistemas de prevención, investigación y con inteligencia antidelincuencial siempre en el marco del respeto y la protección de los derechos.

El compromiso de la misión de la Policía Nacional del Ecuador se funda en el trabajo profesional de los servidores policiales cuando éstos prestan un servicio efectivo y cuando existe el respeto a los derechos humanos de su parte; esto se nota en la transparencia, confianza, credibilidad y legitimidad que tienen ante las personas que protegen. (Dirección Nacional de Planificación y Gestión Estratégica, 2021)

1.1.2. Subsistemas de la Policía Nacional

Como se mencionó, la Policía Nacional del Ecuador es una institución que "protege los derechos, las libertades y las garantías de toda la ciudadanía y cuya misión es la seguridad ciudadana, el orden público, la protección interna y la protección del libre ejercicio de los derechos de las personas que habitan el territorio nacional"; para esto, la Policía Nacional del Ecuador consta de una estructura organizacional que abarca cada uno de los departamentos que se encargan de realizar todas las actividades que les han sido encomendadas a la institución.

La estructura organizacional de la Policía Nacional del Ecuador está establecida en el Estatuto Orgánico de Gestión Organizacional por procesos de la Policía Nacional que fue emitido en mayo de 2019, esta estructura se divide en cuatro áreas: El Comando General, la Gestión General de Seguridad Ciudadana y Orden Público, la Gestión General de Investigaciones y la

Gestión General de Inteligencia Policial; y cada una de estas áreas contiene subdivisiones que a su vez contienen departamentos que gestionan otras áreas referentes a estas subdivisiones.

1.1.3. Competencias Institucionales

En primer lugar, hay que comprender que la competencia que se le otorga a cualquier entidad del Estado está establecida en la ley pues se rige, principalmente, por el principio de legalidad, mismo que se constituye como un principio fundamental dentro del derecho público; este principio menciona que debe existir un sometimiento del poder público hacia la voluntad de la ley dando paso a que exista la denominada "seguridad jurídica"; por lo tanto, se entiende que la competencia establecida a cualquier entidad estatal como es el caso de la Policía Nacional del Ecuador, debe encontrarse en la ley y no puede salirse de ese límite. (Teodorico, 2020)

El Código Orgánico de las Entidades de Seguridad Ciudadana y Orden Público en su artículo 21 habla sobre el sistema de competencias y menciona que las entidades que son reguladas por este código deberán desarrollar sus actividades según "el sistema de competencias coordinado e integral, definido por la autoridad rectora en asignación de competencias que contemple las respectivas funciones y ámbitos de acción, así como la articulación entre éstas". Menciona, también, que cualquier gestión será asignada tomando en cuenta las competencias personales y profesionales de los servidores de cada entidad.

Por otro lado, el artículo 61 del mismo Código establece que la Policía Nacional tiene 19 funciones específicas. Para la presente investigación, las funciones más relevantes son:

- Implementar planes, programas y proyectos para la seguridad ciudadana, protección interna y orden público;
- Servir a la comunidad y proteger a todas las personas;

- Desarrollar acciones operativas para la protección de derechos; mantenimiento, control y restablecimiento del orden público; prevención de las infracciones y seguridad ciudadana;
- Proponer directrices y estrategias de seguridad ciudadana;
- Impulsar y facilitar la participación comunitaria en seguridad ciudadana, protección interna y mantenimiento del orden público y seguridad;
- Cumplir con el control operativo en los ámbitos requeridos de la seguridad ciudadana, protección interna y orden público;
- Apoyar en el control de las organizaciones de vigilancia, seguridad y servicios de investigación privados;
- Prevenir e investigar la delincuencia común y organizada, nacional y transnacional;
- Proteger los derechos de las personas en especial de los grupos de atención prioritaria;
- Proteger a personas incluidas en el sistema nacional de protección de víctimas y testigos.

Así, una vez conocido lo que dice la ley, que regula a las entidades de la seguridad ciudadana y el orden público, sobre las competencias y funciones de la Policía Nacional del Ecuador se entiende que, por el propio principio de legalidad, éstas deben cumplirse y no pueden salirse de esos límites para precautelar la propia seguridad de las personas que habitan en el Ecuador y precautelar también el orden en las actividades diarias que estas realizan.

1.1.4. Tareas Del Sistema Policial

La Policía Nacional del Ecuador tiene una estructura organizacional con departamentos encargados de realizar actividades que le corresponden a la institución para cumplir con sus fines. Esta estructura, se divide en: El Comando General, la Gestión General de Seguridad Ciudadana y Orden Público, la Gestión General de Investigaciones y la Gestión General de Inteligencia Policial en donde, cada una de estas áreas contiene subdivisiones por departamentos.

Para fines investigativos se establecerá lo que hace cada subdivisión de las que se consideraron como más relevantes y concordantes con el tema.

- **Comando General:** Debe dirigir la gestión estratégica, técnica, normativa y administrativa de la Institución para que pueda cumplir con su misión. Se subdivide en
- **Gestión Nacional de Comunicación Organizacional y Estratégica:** Encargada de realizar directrices en la comunicación de la institución para coadyuvar su desarrollo y mejoramiento a través del desarrollo del Plan Estratégico y la solución de problemas de comunicación interna y externa. Esta área, a su vez, se subdivide en la Gestión Nacional de Comunicación organizacional y estratégica que ayuda a coadyuvar la gestión de comunicación tanto organizacional como estratégica para que exista confianza en la ciudadanía hacia la Institución; la Gestión de medios institucionales sirve para fortalecer la imagen institucional y así lograr una buena cultura organizacional; la Gestión de comunicación interna sirve para desarrollar estrategias, acciones y procesos de información, participación e integración institucional interna para que exista una buena cultura organizacional; y la Gestión de comunicación externa sirve para para desarrollar estrategias, acciones y procesos de información, participación e integración institucional, pero de carácter externo para que exista un posicionamiento positivo de la institución.
- **Gestión Nacional de Tecnologías de la Información y Comunicación:** Encargada de asesorar y promover la innovación y el desarrollo tecnológico de la institución esto, tomando en cuenta las tecnologías de la información y comunicaciones en el marco nacional. Se subdivide en Gestión Nacional de Tecnologías de la Información y Comunicaciones cuyo fin es el de coordinar, supervisar, monitorear los planes, proyectos y programas, y evaluar el impacto de las políticas tecnológicas de la institución; la Gestión

de Desarrollo e Innovación que tiene como fin el elaborar y realizar estudios sobre el desarrollo de los sistemas y de los servicios tecnológicos; la Gestión de Operaciones y Soporte Tecnológico se encarga de dirigir, coordinar y gestionar la implementación y mantenimiento del equipamiento tecnológico; la Gestión de Administración del Sistema e Infraestructura se encarga de administrar y operar todos los servicios, los sistemas, las plataformas y la infraestructura tecnológica asegurando su disponibilidad, integridad y confiabilidad; y la Gestión de Seguridad de las TIC´s cuyo fin es el de optimizar la disponibilidad, la capacidad, la efectividad y la continuidad de toda la infraestructura tecnológica a través de actividades que puedan permitir la protección, el monitoreo y la auditoría de la administración y manejo de los recursos y de los procesos de las TIC's en la Policía Nacional del Ecuador.

- **Gestión Nacional de Análisis de Información:** Encargada de analizar los factores que generan la inseguridad, esto lo hacen a través de la sistematización de la información, del estudio y del desarrollo científico para realizar operaciones policiales que cumplan con la seguridad ciudadana y el orden público. Se subdivide en Gestión Nacional de Análisis de Información que es la encargada de coordinar y realizar procesos operativos en todos los departamentos de la Dirección Nacional de Análisis de Información del Delito de los subsistemas policiales; la Gestión de Sistematización de la Información que se encarga de la generación y del mantenimiento de las bases de datos confiables y oportunas que ayudan al análisis, evaluación y toma de decisiones de estrategias que sirvan a la seguridad ciudadana; la Gestión de Control de Análisis de la Información que es la responsable de controlar, monitorear y de evaluar la ejecución de metodologías que ayuden al análisis de la información del delito en los departamentos de Dirección Nacional de Análisis de

Información y de los subsistemas policiales; y la Gestión de Estudio de la Información e Investigación que tiene como fin el analizar la información según las metodologías que se establezcan para poder conocer la problemática delictual y poder establecer estrategias que ayuden a la seguridad ciudadana.

- **Gestión General de Seguridad Ciudadana y Orden Público:** Dirige operaciones del subsistema preventivo y coordinar junto con los subsistemas investigativo y de inteligencia para ayudar a la seguridad ciudadana y al orden público. La única subdivisión relevante es la de la Jefatura de Inteligencia policial pues su fin es el de generar inteligencia para la seguridad ciudadana y orden público, para la asesoría de la toma de decisiones del mando de la institución y otros organismos del Estado tanto a nivel zonal como sub zonal.
- **Gestión General de Investigaciones:** Dirige todos los componentes investigativos en el subsistema de investigación. Se subdivide en Gestión Nacional de Ciberdelito quien se encarga de detectar, identificar, demostrar y neutralizar conductas delictivas en el uso de las TIC's en todas sus modalidades aplicando técnicas y herramientas científicas de investigación digital y Gestión Nacional de Registros y Sistemas Especializados que tiene como fin el obtener, registrar, analizar y comparar elementos balísticos, muestras biométricas y datos para identificar a una persona, además de registrar a los servidores públicos y personas que privadas que porten armas de fuego por medio de los sistemas tecnológicos especializados.
- **Gestión General de Inteligencia Policial:** Dirige los componentes de inteligencia en el subsistema de inteligencia policial para asesorar en las decisiones a favor de la seguridad ciudadana y el orden público. Se subdivide en:

- **Gestión Nacional de Análisis y Producción de Inteligencia:** Encargada de analizar información y extender productos de inteligencia de carácter estratégico, táctico, operacional y prospectivo mediante el procesamiento de información de la Dirección General de Inteligencia.
- **Gestión Nacional de Ciberinteligencia:** Genera operaciones de inteligencia por el riesgo en el ciberespacio que puede existir y llegar a afectar la seguridad ciudadana y el orden público, a través de las herramientas de las TIC´s coordinados junto a los subsistemas policiales.
- **Gestión Nacional de Inteligencia Policial:** Ejecuta actividades de inteligencia a partir de la búsqueda, obtención, sistematización de información de riesgos, amenazas o vulnerabilidades que pueden llegar a afectar al Estado y poder tomar decisiones que ayuden a la seguridad ciudadana y el orden público. A su vez se subdivide en la Gestión Nacional de Inteligencia Policial quien busca coordinar y realizar actividades de inteligencia para los riesgos, amenazas y vulnerabilidades oportunamente; la Gestión de Coordinación Operacional que es la encargada de planificar, coordinar, organizar y evaluar operaciones policiales realizadas en las direcciones nacionales y demás niveles desconcentrados; la Gestión Nacional de Inteligencia Transnacional que se encarga de realizar inteligencia sobre amenazas transnacionales para tomar decisiones en los subsistemas policiales y demás organismos de seguridad del Estado y buscar solución a la seguridad ciudadana y orden público; y la Gestión Nacional de Inteligencia de Seguridad Ciudadana y Orden Público que está encargada de generar inteligencia para prevenir delitos y tomar decisiones en los subsistemas policiales y demás organismos del Estado de seguridad.

Hay que entender que la Gestión más relevante es la de Nacional de Tecnologías de la Información y Comunicación pues en esta gestión aquí nace La Dirección Nacional de Tecnologías de la Información y Comunicación de la Policía Nacional del Ecuador cuyo objetivo operativo es el de:

> Incrementar la prestación y despliegue de servicios tecnológicos de calidad a nivel nacional mediante la automatización de procesos sistematizados, fortalecimiento de la infraestructura tecnológica de los Data Center, soporte y mantenimiento del equipamiento tecnológico, aplicación de normas y/o políticas de seguridad de la información y capacitación de TIC´s. (Dirección Nacional De Tecnologías De La Información Y Comunicación, 2021)

Y su misión es la de:

> Asesorar y promover la innovación y desarrollo tecnológico institucional, respecto a las tecnologías de la Información y Comunicaciones (TIC's) a nivel nacional. Dentro de las atribuciones y responsabilidades de la Dirección Nacional de Tecnologías de la Información y Comunicación esta el Asesorar al Comandante General y dependencias policiales en la planeación, diseño, promoción, desarrollo, implementación y administración de las tecnologías de la información y la comunicación, para el mejoramiento continuo del servicio policial, entre otros. (Dirección Nacional de Tecnologías de la Informaicón y Comunicación, 2022).

1.2. Seguridad Ciudadana y Protección de Datos Personales

1.2.1. Seguridad Ciudadana

La seguridad ciudadana está enmarcada en el respeto a los derechos de la ciudadanía, que debe procurar una convivencia pacífica y en donde la participación de los ciudadanos juega un rol

fundamental pues permite mantener una comunicación bilateral con las autoridades y los actores de la sociedad para conocer las problemáticas del entorno y generar soluciones. (Quintero, 2020).

"La policía es el reflejo de las sociedades y de los sistemas políticos en los que se constituye y funciona" (Sain, 2009). En gran parte de Latinoamérica, histórica y tradicionalmente, los policías se basaron doctrinal, organizacional y funcionalmente según parámetros que resultaban de un proceso histórico en donde fueron introducidas hacia un sistema de "seguridad nacional" como una instancia central del Estado, es decir que resultaron de un grupo de tendencias históricas; dos tendencias fueron las relevantes para llegar al sistema de "seguridad nacional", por un lado, en los regímenes autoritarios las Fuerzas Armadas asumieron el control sobre los policías y los colocaron como piezas que colaboraban con el control y disciplinamiento represivo interno. Por otro lado, en los regímenes democráticos las gestiones gubernamentales fueron indiferentes al desarrollo y dirección de la policía, así, les dieron a las instituciones policiales soberanía política para que pudieran atender cuestiones relacionadas a la "seguridad pública", estas cuestiones eran, por ejemplo, el análisis de la situación de conflictos y delitos, el diseño y conformación de la estructura de la institución policial, el análisis de la modalidad de intervención y los medios en conflictos y delitos, la evaluación de los resultados, los vínculos con otros sujetos institucionales, etc.; todo esto constituyó un gobierno de la seguridad. (Sain, 2009)

La Constitución del Ecuador en su artículo 158 menciona que la seguridad ciudadana se configura como una garantía institucional de las Fuerzas Armadas y la Policía Nacional pues son instituciones que protegen los derechos, las libertades y las garantías de la ciudadanía.

Hay que entender que existen muchas circunstancias que pueden llegar a poner en peligro la seguridad ciudadana y alterar el orden público, lo que hace necesario que intervengan las instituciones de seguridad como la Policía Nacional del Ecuador quien está preparada para el

ejercicio de sus funciones dentro de los límites de su competencia para que, así, puedan garantizar el ejercicio de su misión principal (la seguridad ciudadana y el orden público) siempre tomando en cuenta los estándares del derecho internacional y de los derechos humanos. (Benavides, Benavides, Santillán; 2021)

1.2.2. Protección de Datos

En primer lugar, hay que entender que, según Ana Brian (2006):

> La protección de datos personales es un derecho fundamental de las personas, un derecho de nueva generación que forma parte de lo que la doctrina ha denominado cuarta generación de derechos humanos. Se encuentra especialmente vinculada con las nuevas tecnologías y con la globalización, con la libertad de expresión en la red y la libre circulación de información, con el acopio vertiginoso de información, con el manejo o manipulación de la información y también con la democratización en el acceso a la información.

Este derecho apareció gracias a la evolución del derecho a la intimidad, que luego propició el derecho a la privacidad para finalmente constituirse como un derecho autónomo (a la protección de datos) en sentencia dictada por el Tribunal Federal Alemán de 1983.

Así, se entendería que, al hablar de protección de datos, se habla de una determinación referida a un derecho humano inherente a todas las personas. (Nahabetián, L. 2020)

Es importante, tomar en cuenta que el derecho a la protección de datos personales tiene fundamento y origen en el poder que tiene el titular de disponer de los mismos y que estos sean utilizados para un tratamiento específico; por tanto, quien trata los datos personales debe hacerlo con responsabilidad, control y respeto a los derechos de la persona de quien está tratando los datos.

Entonces, se entendería que el respeto a la dignidad de la persona se relaciona con la protección de datos pues es una garantía a su persona. (Nahabetián, L. 2020)

1.2.3 Naturaleza De La Ley Orgánica De Protección De Datos Personales

En primer lugar, esta ley tiene como objeto y finalidad el garantizar el que se cumpla con el ejercicio del derecho a la protección de datos personales esto en un ámbito de acceso, decisión y protección de los datos; la ley se aplica para dar tratamiento a los datos que se encuentran en cualquier tipo de soporte; para esto, los integrantes del sistema de protección de los datos personales son: el titular de los datos, el responsable del tratamiento de estos, el encargado del tratamiento, existe también un destinatario, una autoridad de protección de datos personales y un delegado de protección de datos personales. los integrantes más relevantes, en el ámbito de la presente investigación, son el titular que es la persona sobre la cual puede existir una vulneración, la autoridad y delegado de protección de datos personales pues es a ellos a quienes se debe acudir para notificar cuando haya existido una vulneración o para prevenir un riesgo si lo hubiera.

Se menciona, por otro lado, en el artículo 7 que, para que se pueda tratar de manera legítima y lícita a los datos personales se debe cumplir con que se protejan los intereses vitales (vida, salud y la integridad) del interesado o de otra persona natural, y, por otro lado, en su artículo 9, menciona que este tratamiento va a tener un interés legítimo en el caso de que la Autoridad de Protección de Datos requiera que se emita un informe de riesgo para proteger los datos, mismo que ayudará a la verificación de amenazas hacia los titulares de los datos y hacia sus derechos fundamentales; así, se deduce que fuera de estos preceptos que son los que sirven a la investigación, el tratamiento de datos y el interés que se pueda llegar a tener de estos ya sea por los integrantes del sistema de protección de datos personales o por terceros se considerará ilícito e ilegítimo, generando un riesgo y una vulneración de los datos personales.

Ahora bien, en cuanto a los derechos que surgen hacia los datos personales hay que entender que el titular puede pedir que se eliminen sus datos cuando el tratamiento afecte sus derechos fundamentales o sus libertades individuales, sin embargo, hay una excepción cuando se trata de que los datos son necesarios para proteger su propio interés vital o el de otra persona natural; por lo tanto, si existiere la eliminación u otro tratamiento de los datos fuera de estos límites se habla de una ilegitimidad y, de la misma manera que en los preceptos anteriores, de un riesgo para los datos personales del titular. En la misma línea, cuando se trata de la transferencia o del acceso a los datos personales solo se pueden realizar si es para el cumplimiento de fines relacionados a las causales de legitimidad que están establecidas en la ley y con consentimiento del titular porque en caso contrario, los datos personales se encontrarán expuestos a riesgos.

Los datos personales deben encontrarse bajo un sistema de seguridad, para esto el responsable o encargado del tratamiento de estos datos debe poner en práctica un proceso de verificación, evaluación y valoración permanente de las medidas de carácter técnico, organizativo y demás para poder garantizar la seguridad de los datos y mejorar su tratamiento. En el caso de que la persona corra cualquier tipo de riesgo, el responsable o encargado del tratamiento de los datos debe implementar medidas como la anonimización, seudonomización o cifrado de datos y cualquier otra que mantenga la confidencialidad, disponibilidad permanente y acceso de datos de forma rápida en caso de que ocurriese algún incidente. Además, el mecanismo gubernamental de seguridad de la información debe abarcar y aplicar para todas las instituciones del sector público, entre ellos la Policía Nacional del Ecuador, un tratamiento que enfrente cualquier tipo de riesgo, amenaza, vulneración, acceso no autorizado, pérdida, alteración, destrucción o comunicación ilícita.

Una de las cuestiones más relevantes, es el hecho de que el responsable del tratamiento de los datos personales debe notificar si llegase a existir una vulneración a la Autoridad de Protección de Datos Personales y la Agencia de Regulación y Control de Telecomunicaciones hasta que se cree la entidad responsable; misma notificación que le debió ser advertida previamente por la entidad encargada. Esta notificación debe hacerse lo más pronto posible (máximo cinco días) si es que la violación a la seguridad se considera un riesgo para los derechos y libertades de la persona.

Ahora bien, luego de haber analizado de manera general la ley, hay que conocer en detalle su ámbito de aplicación pues de aquí surge la problemática de la investigación.

En primer lugar, hay que entender que "ámbito de aplicación" según el Diccionario Panhispánico del Español Jurídico (2017), se define como "el sujeto obligado por lo establecido en una norma jurídica, u objetivo o fin perseguido por ella", así mismo, menciona que se puede referir, también, al "territorio al que se aplica una norma jurídica"; por tanto, para fines de la investigación, se definirá al ámbito de aplicación como aquél ámbito en el que actuará la Ley Orgánica de Protección de Datos Personales según el objetivo que persigue, dentro del territorio ecuatoriano, en el espacio en que se apliquen o se usen los datos personales.

Este ámbito de aplicación material se encuentra establecido en el artículo 2 de la ley y menciona que ésta misma ley va a aplicarse en el tratamiento de datos personales, mismos que estarán contenidos en cualquier tipo de soporte y que se aplicará también a toda modalidad de uso posterior. Sin embargo, menciona que la ley no será aplicable a 7 casos específicos, de los cuales el literal e es el relevante en la investigación y menciona que la ley no se aplicará a:

> Datos personales cuyo tratamiento se encuentre regulado en normativa especializada de igual o mayor jerarquía en materia de gestión de riesgos por desastres naturales; y, seguridad y defensa del Estado, en cualquiera de estos casos deberá darse cumplimiento

> a los estándares internacionales en la materia de derechos humanos y a los principios de esta ley, y como mínimo a los criterios de legalidad, proporcionalidad y necesidad (Ley Orgánica de Protección de Datos Personales, 2021).

Analizando este literal primero mencionaremos a *"datos personales cuyo tratamiento se encuentre regulado en normativa especializada de igual o mayor jerarquía"* esto se refiere a que los datos que se exceptúan de la Ley Orgánica de Protección de datos Personales se encuentran regulados en otras Leyes de carácter "orgánico" (esto en cuando a igual jerarquía) o que se encuentran en la propia Constitución de la República o normativa de carácter internacional (esto en cuanto a mayor jerarquía) según el artículo 225 que menciona que el orden jerárquico de las leyes será en primer lugar la Constitución, luego los tratados y convenios internacionales, luego las leyes orgánicas y demás leyes.

Luego en la parte de *"en materia de gestión de riesgos por desastres naturales; y, seguridad y defensa del Estado"* se entiende que la parte de "seguridad del Estado" es el tema a centrarse y como se conoce, esta seguridad del Estado se ejerce por la Policía Nacional del Ecuador al "atender a la seguridad ciudadana y el orden público y en el proteger el libre ejercicio de los derechos" esto según su misión fundamental establecida en la Constitución de la República del Ecuador en su artículo 163. Hay que tener en cuenta que los conceptos de seguridad y defensa que están inmersos en el Estado se refieren a las fuerzas policiales (Policía Nacional del Ecuador) encargadas de brindar seguridad interna y a las fuerzas armadas encargadas de brindar seguridad externa y además defensa al Estado. Ahora bien, en el papel del Estado pueden existir discusiones sobre los límites de esta seguridad interna y externa pues es un tema confuso ya que es complicado de operar e, incluso, fue tema de discusión (en la consulta popular de febrero de 2023) el otorgar atribuciones de las fuerzas policiales a las fuerzas militares, así la Corte afirmó:

> A priori, la policía nacional es la institución llamada a brindar protección interna y el mantenimiento del orden público en el país; empero, esta tarea no está destinada exclusivamente a un órgano en particular, sino que debe ser entendida desde una perspectiva sistemática e integral. Así, la propuesta intenta viabilizar de manera efectiva que otra institución del Estado, fuerzas armadas, de manera complementaria coadyuve a mantener una seguridad integral dentro del territorio ecuatoriano.; aquello permite un mejor desempeño en cuanto a la protección de este objetivo estatal. (Dictamen No. 001-14-DRC-CC de 31 de octubre de 2014)

Ahora bien, hay que entender, también, que la Constitución de la República menciona a un sistema de seguridad que contiene subsistemas de seguridad como la seguridad ciudadana, la seguridad económica, etc., es decir que existen dimensiones dentro del sistema de seguridad, pero, además, cada subsistema de seguridad debe tener una entidad rectora nombrada por el presidente de la república y es el poder político quien ejerce control y supervisión sobre las actividades que realizan. El subsistema que interesa a la investigación es el de seguridad ciudadana del cual se encarga la Policía Nacional del Ecuador y es aquella política del Estado que se necesita, para poder fortalecer y modernizar, ciertos mecanismos que garantizan Derechos Humanos como el vivir libre de violencia, la protección de las víctimas y de la ciudadanía en general, la vida digna y por tanto el mejoramiento de la calidad de la misma. (Ministerio del Interior del Ecuador, 2019).

Por otro lado, para la protección de esta seguridad del Estado se crea, entonces, el Sistema de Seguridad Pública y del Estado en donde forman parte todas las instituciones que se encargan de la seguridad del Estado cuya finalidad es asumir la seguridad de manera integral consolidando todas sus competencias y responsabilidades para poder enfrentase a todos los problemas de seguridad existentes. En este Sistema de Seguridad Pública y del Estado la institución responsable

de la seguridad ciudadana es, como ya se conoce, el Ministerio del Interior y, como ya se ha mencionado antes, la unidad ejecutora de la misma es la Policía Nacional del Ecuador. (Dávila, Godoy; 2020)

La tercera parte es la de *"deberá darse cumplimiento a los estándares internacionales en la materia de derechos humanos"*, estos estándares se definen como pronunciamientos realizados por organizaciones intergubernamentales y demás organismos de derechos humanos para implementar los derechos humanos plenos a nivel internacional; sin embargo, los estándares serán analizados en un capítulo posterior.

La cuarta parte es *"a los principios de esta ley"*, estos principios se encuentran establecidos en el artículo 10 de la Ley Orgánica de Protección de Datos y, conceptualizados a breves rasgos, son los siguientes:

- **Juridicidad. -** Los datos personales deben estar apegados y cumplir con los principios, derechos y obligaciones de la Constitución, instrumentos internacionales, la presente Ley, su Reglamento y demás normativa y jurisprudencia aplicable.
- **Lealtad. -** El tratamiento de datos personales deberá ser leal. Debe quedar claro a los titulares el trato de datos personales que les conciernen al igual que las formas en que dichos datos son o serán tratados.
- **Transparencia. -** El tratamiento de datos personales será transparente. Toda información relativa al tratamiento será fácilmente accesible y fácil de entender (lenguaje sencillo y claro).
- **Finalidad. -** Las finalidades del tratamiento serán explícitas, legítimas y comunicadas al titular; no podrán tratarse con fines distintos para los cuales fueron recopilados, a menos

que se establezca una de las causales que habiliten un nuevo tratamiento según lo señalado en la ley.

- **Pertinencia y minimización de datos personales. -** Los datos personales deben ser pertinentes y estar limitados a lo estrictamente necesario para cumplir la finalidad del tratamiento.
- **Proporcionalidad del tratamiento. -** El tratamiento será adecuado, necesario, oportuno, relevante y no excesivo según las finalidades para las cuales hayan sido recogidos o a la naturaleza misma de los datos.
- **Confidencialidad. -** El tratamiento de datos personales debe concebirse sobre el debido sigilo y secreto y no debe tratarse o comunicarse para un fin distinto al que fueron recogidos.
- **Calidad y exactitud. -** Los datos personales deben ser exactos, íntegros, completos, comprobables, claros; y debidamente actualizados; para no alterar la veracidad del tratamiento.
- **Conservación. -** Los datos personales se conservarán durante un tiempo no mayor al necesario para cumplir con la finalidad del tratamiento.
- **Seguridad de datos personales. -** Los responsables y encargados del tratamiento de datos personales implementarán las medidas de seguridad adecuadas y necesarias para proteger los datos de cualquier riesgo, amenaza, vulnerabilidad, según la naturaleza de los datos, el ámbito y el contexto.
- **Responsabilidad proactiva y demostrada. -** El responsable del tratamiento de datos personales deberá acreditar el que haya implementado mecanismos para la protección de datos personales. Y está obligado a rendir cuentas sobre el tratamiento.

- **Aplicación favorable al titular. -** En caso de duda sobre el alcance de las disposiciones del ordenamiento jurídico o contractuales sobre la protección de datos personales, los funcionarios judiciales y administrativos las interpretarán y aplicarán en el sentido más favorable al titular de los datos.
- **Independencia del control. -** Para que el derecho a la protección de datos personales sea efectivo la Autoridad de Protección de Datos debe ejercer un control imparcial y autónomo y llevar a cabo acciones de prevención, investigación y sanción.

Y la última parte es *"como mínimo a los criterios de legalidad, proporcionalidad y necesidad",* estos criterios, al igual que los estándares internacionales, serán analizados en un capítulo posterior.

Por otro lado, cabe resaltar lo que dice el artículo 11 de la misma Ley pues su contenido es importante a la investigación. Menciona que:

> Los datos personales cuyo tratamiento se encuentre regulado en normativa especializada en materia de ejercicio de la libertad de expresión, sectores regulados por normativa específica, gestión de riesgos, desastres naturales, seguridad nacional y defensa del Estado; y, los datos personales que deban proporcionarse a autoridades administrativas o judiciales en virtud de solicitudes y órdenes amparadas en competencias atribuidas en la normativa vigente, estarán sujetos a los principios establecidos en sus propias normas y los principios establecidos en esta Ley, en los casos que corresponda y sea de aplicación favorable. En todo caso deberá darse cumplimiento a los estándares internacionales en la materia de derechos humanos y a los principios de esta ley, y como mínimo a los criterios de legalidad, proporcionalidad y necesidad.

Por tanto, se observa que el contenido del este artículo ratifica lo analizado en el ámbito de

aplicación pues al tratarse de datos personales excluidos de la aplicación de la Ley Orgánica de Protección de datos (como el literal e que es motivo de investigación) se debe buscar la aplicación del tratamiento tomando en cuenta otras vías: Estándares Internacionales, los principios de la misma Ley y Criterios de Legalidad, Proporcionalidad, Necesidad e Idoneidad.

1.2.4 Seguridad Ciudadana Excluida Del Ámbito Material De La Ley Orgánica De Protección De Datos Personales

Ahora bien, como se mencionó, la Policía Nacional del Ecuador tiene el deber y la misión de otorgar seguridad ciudadana dentro del Estado al que sirven, sin embargo, la seguridad ciudadana también puede verse afectada cuando existe una vulneración a la seguridad de los datos personales de los servidores policiales, esto puede ocurrir cuando la base de datos de la Dirección Nacional de Tecnologías y Comunicaciones de la Policía Nacional es hackeada pues se puede llegar a conocer concretamente el estado en el que está ese servidor policial, así, si existiese una vulneración a los datos personales de los servidores públicos, tanto su misión de brindar seguridad ciudadana como sus derechos y libertades individuales se verían afectados y no podrían ser regulados por la Ley Orgánica de Protección de Datos Personales ya que resulta en la causal de exclusión de su ámbito de aplicación (artículo 2) establecida en el literal e; por lo tanto, se debe buscar una guía que recolecte lo que los estándares internacionales, los criterios de legalidad, proporcionalidad, idoneidad y los principios de la propia ley digan respecto de estas excepciones para el bienestar tanto de la seguridad del Estado y con ello la seguridad ciudadana (llevada a cabo por la Policía Nacional del Ecuador) como de los derechos y libertades de los servidores policiales.

CAPITULO 2

2.1 Estándares De Derechos Aplicados A La Seguridad Ciudadana. (Objeto de Estudio)

Como se mencionó anteriormente hay excepciones en la regulación de la Ley Orgánica de Protección de Datos (2021) una de ellas se refería a los datos personales "cuyo tratamiento se encuentre regulado en normativa especializada de igual o mayor jerarquía en materia de gestión de riesgos por desastres naturales; y, seguridad y defensa del Estado" y mencionaba que para estos datos deberá cumplirse con los estándares internacionales en materia de derechos humanos.

Los estándares de derechos humanos se configuran como aquellos pronunciamientos que han hecho organizaciones intergubernamentales y otros organismos de derechos humanos a través de resoluciones, recomendaciones, declaraciones, o decisiones en casos concretos como un esfuerzo para implementar los derechos humanos. Es decir que los estándares de derechos humanos son el paso preparatorio para que se pueda gestar el desarrollo de los derechos humanos plenos. (Casas, 2019)

Ahora bien, respecto a los estándares internacionales que se refieren a la seguridad ciudadana, se encuentra el "Informe de Seguridad Ciudadana y Derechos Humanos" que hace la Comisión Interamericana de Derechos Humanos, en donde realiza recomendaciones generales mencionando que: Deben asumir el cumplimiento de las obligaciones internacionales acerca de la protección de los derechos humanos relacionado con la seguridad ciudadana, esto lo logra a partir de la creación y la implementación de políticas públicas integrales que realicen acciones específicas y planes estratégicos en un ámbito operativo, normativo y preventivo del tema; menciona también que debe generar una capacidad institucional en el sector público para poder ejecutar las políticas públicas de seguridad ciudadana, esto deben hacerlo disponiendo de recursos adecuados, tanto técnicos, como económicos y humanos; se debe buscar también que exista una buena formación y selección para quienes integran las institucionales que brindan seguridad social (como las fuerzas policiales) para que se cuente con un servicio de calidad; también se debe buscar

el que se adecuen las normas internas y todo el aparato estatal a la seguridad ciudadana para así asegurar su gobernabilidad y por último se debe realizar procedimientos que ayuden a la efectivización de la rendición de cuentas de todas las autoridades que son responsables sobre la seguridad ciudadana. (Comisión Interamericana de Derechos Humanos, 2009).

Ahora bien, para fines de la investigación también se debe tomar en cuenta a los estándares internacionales de seguridad informática para esto, el más alto estándar internacional de protección de datos es la Guía de Gastón de Riesgos de la Agencia Española de Protección de Datos. Un documento guía que ayuda a la gestión de los riesgos de derechos y libertades y que se puede aplicar a cualquier tratamiento de datos y que además incorpora guías necesarias para realizar una Evaluación de Impacto para la Protección de Datos (EIPD). (Agencia Española de Protección de Datos, 2021)

El objetivo de esta guía es la incorporación de las lecciones aprendidas, los nuevos criterios e interpretaciones que serán aplicadas en la gestión del riesgo para la protección de datos, además, pretende la mejora de materiales que están dirigidos a ayudar al cumplimiento que tienen los responsables dándoles una visión unificada de esta gestión; por otro lado, este documento debe facilitar la integración de la gestión de riesgos para los derechos y libertades en todos los procesos (aplicable a cualquier tratamiento sin importar el nivel de riesgo) de gestión de las entidades.

La gestión de la seguridad de la información contiene modelos de gestión como el Sistema de Gestión de la Seguridad de la Información (SGSI) y directrices como las normas ISO 27000 o ENS que están implementadas y son conocidas lo que hace que se les considere como estándares de seguridad.

Los sistemas de información se constituyen como una proyección hacia los tratamientos de la entidad pues son los medios que dan soporte. Hay que entender, también, que los requisitos de

seguridad en relación a los derechos y libertades son una de las entradas al proceso de análisis de riesgos de los sistemas de información que suelen llegar al departamento de TIC.

Por otro lado, se debe tomar en cuenta la gobernanza de datos, pues, esta sirve para implementar políticas y procedimientos que garanticen una gestión efectiva y eficiente de la información, proyectándose a la gestión de cada uno de los tratamientos de datos. Una de las políticas más necesarias para una organización, es la de la protección de datos para la reducción del riesgo. (Agencia Española de Protección de Datos, 2021)

Cuando se trata de datos personales, la gobernanza de los datos establecida en la organización ha de garantizar el cumplimiento de los derechos y libertades conforme al Reglamento General de Protección de Datos (RGPD). Para ello, los tratamientos de datos personales deben estar respaldados por la implementación efectiva de los principios relativos al tratamiento (art.5 RGPD), tomando las medidas adecuadas y ofreciendo garantías suficientes. En virtud del principio de responsabilidad proactiva, las políticas han de ser compromisos establecidos a nivel de la dirección de la organización.

La implementación de dichas políticas y gobierno de los datos dependerá de la estructura orgánica de cada entidad. Por tanto, la aplicación de políticas de protección de datos supondrá la aplicación de aquellos recursos, procedimientos y controles que pudieran ser necesarios para garantizar dicho cumplimiento en cada entidad concreta. De igual forma tendrán que adoptarse dichas políticas en las organizaciones que pudieran actuar como encargadas del tratamiento con la finalidad de abordar una gestión y control eficaces que garanticen al responsable el cumplimiento del RGPD.

Dichas políticas se deberán verificar, revisar, actualizar y mejorar de forma continua, de acuerdo con los criterios y métodos implantados en la organización

A continuación, se presentarán los pasos que sigue la Guía de Protección de Datos de la Agencia Española, para la gestión de los riesgos para los Derechos y libertades.

Tabla 1

Pasos para la gestión de riesgos para los Derechos y Libertades

I. El Proceso De Gestión Del Riesgo Para Los Derechos Y Libertades
A. Determinación Precisa De Las Finalidades Del Tratamiento
B. Descripción Del Tratamiento
• Análisis A Alto Nivel Del Tratamiento.
• Análisis De Las Fases Del Tratamiento.
• Análisis Del Ciclo De Vida De Los Datos.
• Inventario De Activos.
• Descripción De Casos De Uso.
C. La Evaluación Del Nivel De Riesgo Del Tratamiento Para Los Derechos Y Libertades De Las Personas Físicas
1. Proceso De Evaluación Del Riesgo
2. Identificación Del Riesgo Inherente Y Riesgo Residual
3. Identificación De Los Factores De Riesgo
4. Riesgos De Impacto Muy Elevado
D. El Tratamiento Del Riesgo
1. Clasificación De Las Medidas Y Garantías
2. Establecimiento De La Seguridad Por Defecto
3. Establecimiento Del Ámbito De Las Medidas De Seguridad
E. Implementación De Los Controles, Verificación Y Reevaluación: La Gestión Del Riesgo Como Un Proceso Continuo
II. Políticas De Protección De Datos
III. Identificación Y Análisis De Factores De Riesgo
A. Identificación De Los Factores De Riesgo
B. El Análisis De Los Factores De Riesgo
IV. Evaluación Del Nivel De Riesgo Del Tratamiento
V. Medidas Y Controles Para Disminuir El Riesgo
VI. Valoración Del Riesgo Residual Y Revisión
VII. Evaluación De La Necesidad Y Proporcionalidad Del Tratamiento
VIII. Obligación De Documentación
IX. Recabar La Opinión De Los Interesados O De Sus Representantes
X. Consulta Previa A La Autoridad De Control

Nota: Esta tabla muestra los pasos que sigue la Guía de la Agencia Española de Protección de Datos para la gestión de riesgos de Derechos y Libertades.

Ahora bien, como se conoce, la información se considera un activo importante para el éxito y continuidad en el mercado para cualquier organización, por lo tanto, el aseguramiento de esta información y de los sistemas que maneja la organización y que procesan esta información se constituye como un objetivo primordial para la organización. (Cobarrubias, 2013) En este aspecto, existen otros estándares internacionales que se encargan de la protección de esta información y datos, uno de ellos son las denominadas series ISO/IEC (International organisation for Standardization e International Electrotechnical Commission) que serán definidas a continuación:

- **SERIE ISO 27000.-** Son un conjunto de estándares desarrollados o en desarrollo por ISO/IEC que otorgan un marco de gestión de la seguridad de la información que se puede utilizar para todo tipo de organización
- **ISO/IEC 27001.-** Se trata de la única norma internacional auditable que define y establece los requisitos para un "Sistema de Gestión de Seguridad de la Información" (SGAI). Garantiza la selección de los controles de seguridad para que sean adecuados y proporcionales y así poder proteger los activos de información y poder brindar confianza a las partes interesadas. Busca adoptar un enfoque por procesos en donde pueda establecer, implementar, supervisas, operar, mantener y mejorar un SGSI
- **ISO/IEC 27002.-** Es un programa que ayuda a la certificación de la seguridad de la información, por lo tanto, busca concienciar y prevenir riesgos y no solo se enfoca en soluciones tecnológicas, sino que proporciona una visión amplia acerca de los problemas relacionados con la información de la organización o de cualquier persona que forme parte de ella. Aquí, los profesionales certificados de seguridad de la información ayudan en la

certificación de la organización respecto de las series ISO 27000, ayudan a aplicar habilidades prácticas para que la organización sea consciente sobre la seguridad de la información haciendo que se sienta más responsable y pueda prevenir riesgos, y ayuda, sobre todo, a que se consiga una cultura que se oriente a conseguir una seguridad sobre los datos que maneja la organización.

- **ISO/IEC 20000.-** Se conoce como un estándar reconocido a nivel internacional en la gestión de servicios de las Tecnologías de la Información.
- **ISO/IEC 27701.-** Se configura como un estándar internacional que ayuda al aseguramiento, confidencialidad y la integridad de los datos y la información; además ayuda también a los sistemas que procesan estos datos.

Son estos estándares internacionales los que permiten conocer cómo se debe actuar en la protección de datos personales cuando se trata de datos que vulneren los derechos y libertades de las personas, pero también que puedan llegar a vulnerar con esto, la seguridad del Estado (así como la seguridad ciudadana) poniendo en riesgo a la persona (en el caso de la investigación: al servidor policial) y al aparataje Estatal.

Por lo tanto, el objeto de estudio se encuentra enfocado en el procedimiento que deben seguir quienes protegen los datos cuando existe una vulneración a los datos de los servidores policiales tomando en cuenta que esto vulnera no solo sus derechos y libertades sino que también puede poner en riesgo su trabajo y por tanto la seguridad ciudadana que brindan y la seguridad Estatal, tomando en cuenta que no se regirán por la Ley Orgánica de Protección de Datos sino que buscarán enfocarse en los estándares internacionales mencionados y en criterios de proporcionalidad, necesidad e idoneidad que serán explicados a en el siguiente tema.

2.2. Criterios De Proporcionalidad, Necesidad E Idoneidad

En los datos personales que están exentos de la regulación de la Ley Orgánica de Protección de Datos y que están establecidos en el literal e, se menciona que además de los estándares internacionales se debe tomar en cuenta los criterios tanto de proporcionalidad como de necesidad, criterios que serán expuestos a continuación.

En primer lugar, se debe entender que "criterio" según el diccionario de la Real Academia Española de la Lengua, se refiere a un "juicio", entonces, para fines de la investigación este "juicio" se referirá a un proceso de razonamiento mental más no como como un procedimiento judicial o una decisión que hace un juez porque se conoce que este criterio lo realiza un servidor que no es un juez.

Ahora bien, estos "criterios o juicios" que el literal e menciona se refieren, además, a determinados principios como el de proporcionalidad y necesidad, y hay que entender que estos principios además de ser considerados como criterios de razonamiento mental que ayudan al establecimiento de la decisión del servidor, se consideran constitucionalmente como "mandatos de optimización que se realizan en la mayor medida en que son posibles", son normas no distinguidas por la vigencia absoluta sino por una aproximativa, cuyo objetivo son los derechos y las libertades fundamentales, así como también los bienes jurídicos colectivos. (Cárdenas, 2014).

Se debe entender de qué manera estos principios se configuran en criterios o juicios como una medida de tratamiento para los datos personales que están exentos del ámbito de aplicación de la Ley Orgánica de Protección de Datos Personales, para esto la Guía De Gestión De Riesgos De La Agencia Española De Protección De Datos Personales ha establecido como se debe realizar la evaluación de la necesidad y proporcionalidad del tratamiento de datos personales en cuanto a la finalidad que estos tengan. El supervisor europeo de Protección de datos ha precisado el principio de proporcionalidad que se usa para realizar la ponderación de derechos o bienes jurídicos

protegidos que están en conflicto. Así, este principio llevado a la evaluación de la necesidad y de la proporcionalidad del tratamiento hace que se configure una ponderación que atiende a tres criterios que siguen un determinado orden para que se cumplan correctamente. (Agencia Española de Protección de Datos, 2021)

- En primer lugar, el juicio de idoneidad, aquí hay que determinar si el tratamiento para los datos es el adecuado según la finalidad que se busca perseguir; este tratamiento debe dar respuesta a las carencias, demandas, exigencias, obligaciones o a las oportunidades objetivas que puedan aparecer y, además, el tratamiento puede llegar a conseguir los objetivos que se ha propuesto con eficacia.
- En segundo lugar, se encuentra el juicio de necesidad, aquí se busca la determinación de si la finalidad que se persigue puede o no alcanzarse de algún otro modo que sea menos lesivo o invasivo, es decir, que así se determina que no exista un tratamiento alternativo que sea lo suficientemente eficaz para conseguir el fin que se persigue.
- Por último, el juicio de proporcionalidad en sentido estricto, aquí se establece que la gravedad del riesgo del tratamiento tanto para los derechos como para las libertades, e incluso la intromisión en la privacidad, debe ser la adecuada según el fin que se persigue y esta gravedad, además, debe estar proporcionada a la urgencia de esta. En este criterio se busca ponderar el beneficio que el tratamiento que protege los datos proporciona a la sociedad manteniendo equilibrio respecto del impacto que puede llegar a representar sobre otros derechos fundamentales; en este criterio, además, se debe tomar en cuenta que, aunque se puede ceder parcialmente, en ningún caso se puede establecer una negación absoluta sobre el derecho a la protección de datos.

Luego de esta evaluación se establece una decisión para conocer si debe o no realizarse el tratamiento o si se debiera modificar para que cumpla con los tres criterios (idoneidad, necesidad y proporcionalidad). Hay que entender que este proceso de evaluación ayuda a la identificación de elementos que modifiquen el tratamiento y ayuden que esté acorde a la proporcionalidad, además antes de realizar esta evaluación se debe consultar los análisis de necesidad y proporcionalidad que se haya hecho previamente sobre tratamientos similares y consultar informes jurídicos que ayuden a identificar los límites a los que debe sujetarse el tratamiento. Por otro lado, la guía no recomienda continuar con la Evaluación de Impacto para la Protección de Datos si es que el tratamiento no ha cumplido con la evaluación de la necesidad y proporcionalidad, por lo tanto, el requisito indispensable es que rehaga un análisis completo de las tres dimensiones indicadas. (Agencia Española de Protección de Datos, 2021)

Por lo tanto, el enfoque para el procedimiento a seguir de quienes protegen los datos cuando existe una vulneración hacia los datos de los servidores policiales debe basarse también en estos criterios de proporcionalidad, necesidad e idoneidad.

2.3. Dificultad de aplicar los Estándares y los Criterios en la Ley Orgánica De Protección De Datos Personales. (Problema de Investigación)

Como se expuso anteriormente, los estándares y criterios se aplican cuando los datos no se regulan por la Ley Orgánica de Protección de Datos Personales (2021); así, según su artículo 2 que menciona el ámbito de aplicación y sus excepciones se menciona en el literal e que los datos personales de cierta jerarquía en materia de seguridad nacional y defensa del Estado no entran en los datos que regula la ley, por tanto, se deduce que si se habla de que existe un peligro hacia los derechos fundamentales y libertades individuales de los servidores policiales, estos datos ya no

formarían parte de la regulación de la Ley Orgánica de Protección de Datos pues pueden resultar en vulneraciones tanto para la misión que debe cumplir como para sus derechos y libertades.

Por lo tanto, al existir una dificultad en que la Ley Orgánica de Datos Personales regule estos datos, debe buscarse un nuevo protocolo que los regule cuando exista una vulneración para conocer cómo, cuándo y a quién debe notificarse; pero, siempre tomando en cuenta que no constituya un riesgo a la seguridad de los derechos y libertades de los servidores, así como también a la ciudadanía que protegen; este protocolo o guía deberá recolectar información proporcionada por los estándares internacionales tanto de derechos humanos como de protección de datos personales; también, debe usar criterios de legalidad, proporcionalidad, idoneidad y necesidad; y debe guiarse en los principios establecidos en la propia Ley Orgánica de Protección de Datos Personales para el bienestar tanto de la seguridad del Estado y con ello la seguridad ciudadana como la seguridad de los derechos y libertades de los servidores policiales.

Así, la presente investigación tiene como objeto central realizar un análisis técnico – jurídico de la obligación legal que tiene la Dirección Nacional de Tecnologías de la Información y Comunicación de la Policía Nacional del Ecuador de notificar vulneraciones a la seguridad de datos personales, por lo que se tomará en cuenta la Ley Orgánica de Protección de Datos Personales, Normas Internacionales como La guía de Gestión del riesgo y evaluación de impacto en tratamientos de datos personales de la Agencia Española de Protección de Datos, la normativa ISO27001, ISO27002, ISO27035, ISO9000,ISO27032 y Esquema Gubernamental De Seguridad De La Información, y demás leyes vigentes para determinar si la institución de la Policía Nacional del Ecuador debe notificar estas vulneraciones y el cómo debe hacerlo, para lo cual se ejecutará la investigación mediante técnicas investigativas y, posteriormente, se realizará un análisis en las áreas de conocimiento legal e informático.

2.4. Deber de Notificación de la Vulneración de la Seguridad de Datos Personales a la Autoridad de Protección de Datos Personales. (Pregunta de Investigación)

Como ya se mencionó anteriormente, la Ley Orgánica de Protección de Datos menciona en su artículo 43 que debe existir una notificación si llegase a existir una vulneración de la seguridad, cuyo procedimiento es que el responsable del tratamiento de estos datos (datos que son regulados por esta ley) debe notificarlo a la Autoridad de Protección de Datos Personales y a la Agencia de Regulación y Control de las Telecomunicaciones, y esta notificación se debe hacer lo más pronto posible, es decir que debe tardar como máximo un término de 5 días luego de que se haya tenido constancia de esta vulneración, debe considerarse que esta vulneración a la seguridad se configure como un riesgo para los derechos y libertades de la persona. La norma, también, menciona que si llegase a existir una demora en la notificación y no se la emite en el término de 5 días esta debe indicar los motivos por los que se ha demorado.

Esta notificación debe realizarse, como ya se mencionó, con datos que estén regulados por la ley, sin embargo (y como ya se trató anteriormente) existe en la misma ley un apartado que menciona los datos que no están regulados, entre ellos los datos personales regulados en normativa especializada en materia de gestión de riesgos por desastres naturales; y, seguridad y defensa del Estado; por lo tanto, (y como ya se expuso) si llegase a existir una vulneración a los datos personales de los servidores policiales (Contenidos en la Dirección Nacional de Tecnologías de la Información y Comunicación de la Policía Nacional del Ecuador) que, por motivos de su trabajo, pueden llegar a correr peligro respecto de sus derecho fundamentales y libertades individuales, estos datos ya no formarían parte de la regulación de la Ley Orgánica de Protección de Datos. Así, una vulneración a los datos personales de los servidores públicos es una vulneración a su misión

y a los derechos y libertades individuales de cada uno y por tanto son excluidos de la regulación de la Ley Orgánica de Protección de Datos Personales.

Esto da a entender que el deber de notificación de esta vulneración debe ser pensado adecuada y nuevamente para no correr el riesgo de vulnerar los datos personales de los servidores policiales y con ello vulnerar el trabajo que realizan vulnerando, así, su misión de cumplir con la seguridad ciudadana y del Estado.

Por lo tanto, la pregunta de investigación que cabe es si: La Dirección Nacional de Tecnologías de la Información y Comunicación de la Policía Nacional del Ecuador ¿debe (o no) notificar la vulneración de la seguridad de datos personales que constituyan un riesgo para los servidores policiales Directivo y Técnico Operativos de esta Institución?

2.5. Efectos del problema

Los datos personales se definen como registros u otra información que por sí sola o vinculada con otros datos, puede revelar la identidad de una persona viva. (Álvarez, Escobar, 2022)

En el caso de Ecuador para la protección de datos se ha establecido la Ley Orgánica sobre la Protección de Datos Personales. Así, Ecuador ingresa a una era globalizada en donde resalta la importancia del formato jurídico, para asegurar el ejercicio pleno de los derechos en la evolución del paradigma tecnológico y constitucional (Ordóñez, 2017). Sin embargo, incluso y con los esfuerzos a nivel legal han ocurrido varios ciberataques, esto ha hecho que el Ecuador se ubique en el séptimo lugar dentro de los países de la región como inseguro en donde los delincuentes utilizan diferentes técnicas “como el phishing, spear-phishing, el watering-hole e incluso la infección de infraestructura utilizando todo tipo de malware” (UNIR, 2021).

Se establece, entonces, que cada día la ciberseguridad juega un papel importante en la protección de los derechos fundamentales y libertades individuales; haciendo que la regulación o

protocolización de ciertas áreas del ciberespacio para la protección de la seguridad de datos personales sea necesaria. En especial en el caso de datos personales de servidores policiales que son quienes se encargan de la seguridad ciudadana y el orden público en el Estado pues si la inseguridad en sus datos personales llega a constituir un riesgo para sus derechos fundamentales y libertades individuales se estima que el cumplimiento de su misión también se ve afectada (la seguridad ciudadana y el orden público) y puede provocar una afectación en la seguridad Estatal. Por lo tanto, el establecer protocolos (tomando en cuenta los estándares internacionales y principios básicos como el de legalidad, proporcionalidad, idoneidad y necesidad) para esta problemática es necesaria.

2.6. Causas del problema

El ciberespacio, se puede considerar como "un grupo de equipos electrónicos conectados en redes haciendo uso de software, de datos y de humanos que interactúan de manera global con ellas". (Llorens, 2017) La ciberseguridad, por su parte se configura como aquel conjunto de acciones que busca la protección de la información de toda la comunidad que se encuentra en el ciberespacio (Cornejo, Verdezoto, & Villacís, 2019). Se establece que indistintamente del tipo de ciberataque que ha infectado el sistema informático se entiende que esto acarrea afectaciones en el rendimiento de los computadores, alteración o eliminación de los ficheros, aplicaciones cerradas o ejecutadas sin el consentimiento, el recibir correos que no fueron enviados, la suplantación de identidad, decodificación de contraseñas, denegación de servicio (DoS) y denegación de servicio distribuido (DDoS), incluso ataques combinados. (Cedeño, 2022).

Para el Ecuador, la no existencia de personal capacitado para atender con prontitud y poder hacer frente a los ciberataques, la dificultad para emprender proyectos de cambios tecnológicos y hacer que se integren a plataformas que ya existen o, incluso, la falta de presupuesto para

administrar y reforzar apropiadamente la seguridad, son algunas de las razones que impiden combatir eficazmente los ciberataques. (Cedeño, 2022).

Algunos de los ejemplos que Ecuador ha sufrido respecto de ciberataques son: a) 2018, un ciberataque afectó al sistema de la Agencia Nacional de Tránsito del Ecuador beneficiando ilegalmente a 15.970 usuarios con licencias de conducir provocando un perjuicio de más de un millón de dólares para el estado (El Telégrafo, 2018); b) 2019, Ecuador tomó la decisión de dar por terminado el asilo el a Julián Assange en la embajada ubicada en Londres; provocando que el país sufriera 40 millones de ciberataques (El Comercio, 2019 con la intención de provocar afectación a la infraestructura tecnológica de las entidades del Estado.

Por ello, para mejorar la seguridad en el ciberespacio, se requiere la colaboración entre la empresa privada y el sector público, involucrando además a las ONG´s, a las corporaciones vinculadas con las tecnologías de la información y comunicación y a toda la sociedad en general (Castro & Monteverde, 2018), se requiere, además, del análisis de normativa internacional y la adecuación a la normativa nacional según el contexto actual y las nuevas tecnologías.

En el Ecuador, a pesar de haberse aprobado la Ley Orgánica de Protección de Datos Personales, existen datos que no entran en su ámbito de aplicación y que necesitan de un protocolo para poder ser tratados (que tomen en cuenta los estándares internacionales y principios básicos como el de legalidad, proporcionalidad, idoneidad y necesidad) y así no se llegue a afectar la seguridad ciudadana y el orden público y por tanto no se afecte tampoco la seguridad Estatal.

2.7. Escenarios

Con la presente investigación, al determinar la obligación o no de notificar violaciones de datos personales, se cumpliría con claridad el procedimiento, beneficiando a todos los usuarios de los dos sistemas informáticos existentes en la Dirección Nacional de Tecnologías de la

Información y Comunicación de la Policía Nacional del Ecuador, con la finalidad de proteger a los servidores policiales y garantizando que sus datos están protegidos de robos de identidad, estafas, suplantaciones de identidad, brindando servicios digitales más eficientes, eficaces y sobre todo creando confianza en el tratamiento de los datos personales que maneja este departamento policial.

2.8. Objetivo General

Determinar si la Dirección Nacional de Tecnologías de la Información y Comunicación de la Policía Nacional del Ecuador debe notificar la vulneración de la seguridad de datos personales a través de un análisis técnico-jurídico para comprender si existen (o no) posibles excepciones a esta obligación por el riesgo que puede tener el personal de esta Institución

2.9. Objetivos Específicos

2.9.1. Preguntas específicas de investigación

1. ¿Cuándo debe la Dirección Nacional de Tecnologías de la Información y Comunicación de la Policía Nacional notificar violaciones de datos personales?
2. ¿Cómo debe actuar la Dirección Nacional de Tecnologías de la Información y Comunicación de la Policía Nacional si ha existido una violación de datos personales en la Dirección General de Inteligencia de la Policía Nacional?
3. ¿Cuál es el riesgo de inobservar la protección de datos personales?

2.9.2. Objetivos específicos

1. Examinar cuándo debe la Dirección Nacional de Tecnologías de la Información y Comunicación de la Policía Nacional del Ecuador, notificar la vulneración de la seguridad de datos personales

2. Advertir cómo debe actuar Dirección Nacional de Tecnologías de la Información y Comunicación de la Policía Nacional del Ecuador si ha existido una vulneración de la seguridad de datos personales
3. Identificar cual es el riesgo de inobservar la protección de datos personales de los servidores policiales de la Institución

CAPITULO 3

3.1 Seguridad de Datos Personales

Los datos personales son 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. Así, un dato personal es el dato que hace identificable a una persona natural.

Los datos personales se deben proteger debido a que con ellos se protegen, también, los derechos y libertades de la persona en un mundo globalizado en donde los ataques a la seguridad de la información se han vuelto desmedidos.

Ahora bien, según la ley orgánica de protección de datos personales, el responsable del tratamiento de datos debe adoptar las medidas técnicas y organizativas necesarias para garantizar la seguridad de los datos personales, para evitar su alteración, pérdida, tratamiento o acceso no autorizado contemplando controles que garanticen los tres pilares de seguridad de la información la integridad, disponibilidad, la confidencialidad.

Para Miguel Julio (2015) las medidas de seguridad que debe implantar el responsable se dividen en 3 niveles básico, medio y alto en función del tipo de datos tratado. Además, tomar en cuenta que cuanto mayor sea la afectación respecto a la intimidad de los datos tratados mayor será

el nivel de seguridad y más exigentes las medidas de seguridad que se debe aplicar para su almacenamiento.

Entonces para la seguridad de los datos se debe tomar en cuenta:

1. Antes de obtener el dato realizar un consentimiento firmado donde entre otras cosas se establezca la dirección electrónica a donde se debe notificar cualquier vulnerabilidad,
2. Obtener los datos de calidad (observando minimizidad, exactitud y veracidad),
3. Garantizar de confidencialidad, integridad y disponibilidad siempre.
4. Garantizar la resiliencia de los sistemas y servicios de tratamiento, dotar de la capacidad de restaurar la disponibilidad y el acceso a los datos personales de forma rápida en caso de incidente físico o técnico,
5. La seudonimización y el cifrado de datos personales,
6. Tener políticas tanto jurídicas como técnicas claras de cumplimiento interno para el tratamiento seguro de los datos,
7. Los procesos de verificación, evaluación y valoración regulares de las medidas de seguridad,
8. En caso de afectación o vulneración se deberá notificar
9. De acuerdo con la finalidad para la que fueron recopilados los datos se deberán borrar de forma segura tanto si permanecen en estado físico(papel) o digital.

3.2. Qué tipos de Datos Personales maneja la Policía Nacional del Ecuador y la Dirección Nacional De Tecnologías de la Información y Comunicación

En forma general y confidencial se constató que en la base de datos a cargo de la Dirección Nacional de Tecnologías de la Información y Comunicación se manejan datos personales del

personal Directivo y Técnico Operativo de la policía nacional, en el ámbito personal, educativo, financiero, salud, servicios, entre otros, concernientes a datos del talento humano policial.

Por otra parte, según la Ley Orgánica de Protección de Datos en su artículo 4 y 5, quienes intervienen en el proceso de protección de datos son:

- **Titular:** Persona natural cuyos datos son objeto de tratamiento.
- **Responsable de tratamiento de datos personales:** persona natural o jurídica, pública o privada, autoridad pública, u otro organismo, que solo o conjuntamente con otros decide sobre la finalidad y el tratamiento de datos personales.
- **Encargado del tratamiento de datos personales:** Persona natural o jurídica, pública o privada, autoridad pública, u otro organismo que solo o conjuntamente con otros trate datos personales a nombre y por cuenta de un responsable de tratamiento de datos personales.
- **Destinatario:** Persona natural o jurídica a quien se le comunican los datos personales.
- **Autoridad de Protección de Datos Personales:** Autoridad pública independiente encargada de supervisar la aplicación de la presente ley, reglamento y resoluciones que ella dicte, con el fin de proteger los derechos y libertades fundamentales de las personas naturales, en cuanto al tratamiento de sus datos personales.
- **Delegado de protección de datos**: Persona natural encargada de informar al responsable o al encargado del tratamiento sobre sus obligaciones legales en materia de protección de datos, así como de velar o supervisar el cumplimiento normativo al respecto, y de cooperar con la Autoridad de Protección de Datos Personales, sirviendo como punto de contacto entre esta y la entidad responsable del tratamiento de datos.

Ahora bien, hay que resaltar que para la presente investigación se conceptualizará a los datos sensibles como: aquellos datos personales con los que se pueda hacer uso para la vulneración

de derechos y libertades del servidor policial que además vulnere la misión (seguridad ciudadana y el orden público) que debe cumplir en pro del Estado.

A continuación, se detallan algunos campos como muestra de registros de datos:

Tabla 2

Muestra de Registro de Datos

Diferentes atributos	
IGenPersona	Número de identificación de una persona en una base de datos relacional
iTipoPersonal	Tipo de personal policial (Línea, administrativo, Justicia, sanidad)
iCalidadIngreso	Situación de ingreso a la Institución Oficial o Clase
iPromocion	Numero de promoción a la que pertenece (esto identifica el año de ingreso y el tiempo de servicio)
iTipoSangre	Identifica el tipo de sangre
iOrdenGeneral	Identifica la orden general con la que se le da el alta como servidor policial.
Dirección	Dirección de domicilio de servidor policial
apellido1	Primer apellido(paterno) del servidor policial
apellido2	Segundo apellido (materno) del servidor policial
Nombres	Nombres del servidor policial
Fecha Ingreso	Fecha de ingreso a la institución
Fecha Orden Ingreso	Fecha de publicación de la orden general
Orden General Ingreso	Detalles de la orden general de ingreso
Estatura	Estatura de servidor policial
Talla Calzado	Número de calzado del servidor policial
Talla Gorra	Talla de gorra del servidor policial
Talla Terno	Talla de terno del servidor policial
Numero Afiliación	Numero de afiliación a seguro social del servidor policial
Lugar Nacimiento	Provincia, cantón y dirección de nacimiento del servidor policial
Usuario	Siglas de identificación como usuario en la base de Datos
Fecha	Fecha de creación de los datos
Ip	Protocolo de Internet de donde se ingresó los datos a la DB
Nro. Teléfono celular	Número telefónico de uso del servidor policial.
Nro. Teléfono convencional	Número de teléfono convencional(domicilio) del servidor policial
Cedula	Numero de cedula del servidor policial
Correo	Correo electrónico personal o institucional del servidor policial.

Nota: Esta tabla presenta una muestra de Registro de Datos de los Servidores Policiales que son considerados como los más relevantes y personales.

3.3. Sistema de Seguridad para los Datos

Ahora bien, hay que mencionar que mediante el Acuerdo Ministerial 025-2019 de fecha 20 de septiembre de 2019, firmado por el señor Ministro de Telecomunicaciones y de la Sociedad de la Información MINTEL, la Policía Nacional del Ecuador llevó a cabo la implementación y actualización obligatoria del Esquema Gubernamental de Seguridad de la Información versión N. 2 (EGSIV2), para la toma de decisiones y acciones apropiadas plasmadas en políticas de alto nivel, definiendo el objetivo, dirección, principios y reglas básicas para la gestión de la seguridad de la información, asegurando que los activos de información que genera, administra, transforma y custodia la Policía Nacional estén protegidos de una manera adecuada frente a las amenazas, vulnerabilidades y riesgos a los que podrían estar expuestos tales como por ejemplo fraude, sabotaje, inteligencia, violación a la privacidad, hackers, interrupción de servicio, accidentes y desastres naturales.

En ese documento se describe la política general de seguridad de la Información Institucional, los lineamientos generales, requerimientos legales y las responsabilidades tanto de la alta dirección como de los propietarios de los activos de información y en general todos los servidores policiales y servidores civiles que laboran en la institución, proveedores y terceros que intervengan en la generación, tratamiento, procesamiento, almacenamiento y custodia de la información de la Policía Nacional del Ecuador.

Además, La Policía Nacional del Ecuador declara que la información que genera, utiliza, procesa, comparte, almacena y custodia en medio electrónico o escrito, clasificada como pública, confidencial, reservada, secreta y secretísima, es un activo de alto valor Institucional, así como la infraestructura que la soporta, son esenciales para la continuidad de la labor institucional, para el cumplimiento de su misión constitucional, por lo que es fundamental identificarlos y protegerlos, mediante la aplicación del Esquema Gubernamental de Seguridad de la Información garantizando

la confidencialidad, integridad, y disponibilidad controlando el acceso, uso y disponibilidad, conforme a las leyes y normativa institucional.

La Policía Nacional del Ecuador, se compromete con el establecimiento, implementación, mantenimiento y mejora continua del Sistema de Gestión de Seguridad de la Información (SGSI), que garantice la confidencialidad, disponibilidad e integridad de la información por medio de la gestión de riesgos, incidentes de seguridad y en cumplimiento de los requisitos legales y regulatorios, que exige el Ministerio de Telecomunicaciones y de la Sociedad de la Información, que aplican a las Instituciones de la Administración Pública Central, Institucional y que depende de la Función Ejecutiva, para impulsar el desarrollo de procesos, proyectos y actividades. (Informe de la evaluación de los riesgos, 2020)

3.4. Sistemas de Protección de datos

En el caso de que la persona corra cualquier tipo de riesgo, el responsable o encargado del tratamiento de los datos debe implementar medidas como la anonimización, seudonomización o cifrado de datos y cualquier otra que mantenga la confidencialidad, disponibilidad permanente y acceso de datos de forma rápida en caso de que ocurriese algún incidente

- **Anonimización:** La aplicación de medidas dirigidas a impedir la identificación o reidentificación de una persona natural, sin esfuerzos desproporcionados. (Ley Orgánica de Protección de Datos, 2021)
- **Seudonimización:** Tratamiento de datos personales de manera tal que ya no puedan atribuirse a un titular sin utilizar información adicional, siempre que dicha información adicional, figure por separado y esté sujeta a medidas técnicas y organizativas destinadas a garantizar que los datos personales no se atribuyan a una persona física identificada o identificable. (Ley Orgánica de Protección de Datos, 2021)

La seudonimización se está convirtiendo en una importante técnica de seguridad que proporciona un medio que facilita el tratamiento de datos personales y ofrece, al mismo tiempo, sólidas garantías para proteger los datos personales y, por tanto, salvaguardar los derechos y libertades de las personas.

La seudonimización es una técnica bien establecida que tiene por objeto proteger los datos personales ocultando la identidad de las personas. (La Adopción De Técnicas De Seudonomización, 2022)

- **Cifrado de Datos:** Es convertir datos de texto sin formato (sin cifrar) en texto incomprensible para que se vea como aleatorio, se accede a ellos con una clave de cifrado, además es utilizado como defensa contra ataques, incluidos el malware y el ransomware.

  El cifrado de datos protege los datos digitales transmitidos en el cloud y los sistemas informáticos, también se utiliza para proteger contraseñas.

  A modo de explicación, el cifrado se puede entender como el hecho de guardar algo valioso dentro de una caja cerrada con seguridad, en cambio, el descifrado se puede comparar con abrir la caja y recuperar el elemento valioso.

Se puede emplear la Técnica Generador de seudónimos Contador de función monótona que comienza con un determinado valor que se va incrementando cuando se necesita un nuevo seudónimo (Número aleatorio, Valor aleatorio) extraído entre un límite mínimo y un límite máximo cuando se necesita un nuevo seudónimo: Función resumen (hash); Función criptográfica de un solo sentido (no reversible) que transforma los datos personales de entrada en valores de longitud fija; Código de autentificación de mensaje resumido (HMAC); Función criptográfica de un solo sentido (no reversible) que añade una clave que la hace menos predecible que una función resumen (hash); Cifrado Función criptográfica bidireccional (reversible) que transforma los datos

personales de entrada en valores que pueden volver a transformarse en su formato original utilizando una clave

3.5. Análisis de Riesgo y Evaluación de Impacto (idoneidad, necesidad y proporcionalidad)

En la Dirección Nacional de Tecnologías de la Información de acuerdo al informe de Evaluación de Riesgos, 2020 se ha realizado la identificación de vulnerabilidades y amenazas que afectan a los activos de información, para mejorar la seguridad en la información que la institución gestiona, procesa, almacena y custodia, frente a la gestión y tratamiento de riesgos de seguridad de la información que los activos enfrentan y con ello brindar un insumo para la toma de decisiones mediante un diseño, mantenimiento y mejora continua del sistema de gestión de seguridad de la información por lo que actualmente cuenta con el EGSI V2.

Sin embargo, según la gestión del riesgo y evaluación de impacto en tratamiento de datos personales, 2021 debemos considerar que la evaluación del nivel de riesgo es una tarea del responsable que debe orientarse hacia las operaciones de tratamiento que realiza y no hacia el posible contenido de un fichero de datos.

La evaluación del nivel de riesgo tiene que tener en cuenta todos los aspectos del tratamiento, que se derivan de la naturaleza, ámbito, el contexto y los fines del tratamiento.

Las medidas y garantías a adoptar no se deben limitar a medidas de seguridad, sino que, además, deben implicar medidas sobre la concepción del tratamiento, gobernanza y políticas de protección de datos, medidas de protección de datos desde el diseño (de desvinculación, transparencia y control), gestión de brechas de datos personales y, en su caso, la realización de una EIPD.

En cuanto a la estrategia de cómo afrontar el riesgo, distinguimos medidas orientadas a:

- **Reducir/mitigar el riesgo:** Para reducir el nivel de riesgo, se deben establecer medidas de control que disminuyan los niveles de probabilidad y/o los impactos asociados al riesgo inherente.
- **Evitar/eliminar el riesgo:** Si el riesgo es muy elevado y no se quiere asumir el mismo, se puede decidir abandonar la actividad de tratamiento o, en su defecto, modificar la naturaleza, el alcance, el contexto y la finalidad del tratamiento para evitar dicho riesgo.
- **Aceptar/asumir el riesgo:** Si el riesgo inherente es inferior al nivel de riesgo considerado como aceptable, se puede asumir, pero sin olvidar la necesidad de continuar gestionándolo de forma continua.
- **Atendiendo a su naturaleza, los controles pueden incorporar medidas organizativas:** Medidas asociadas a los procedimientos, a la organización y/o al gobierno de la entidad relacionadas con la aplicación de políticas de protección de datos.
- **Legales:** Garantías jurídicas que pudieran ser necesarias como el establecimiento de cláusulas de confidencialidad o la adopción de compromisos de no reidentificación, entre otros.
- **Técnicas:** Medidas de protección desde el diseño, medidas de seguridad o medidas para auditoría ("accountability") automática, entre otras.

Tabla 3

Gestión del Riesgo para los Derechos y Libertades

Gestión del Riesgo para los Derechos y Libertades				
Proactivas/ preventivas	Garantías legales	Garantías técnicas	Garantías organizativas	Reducir/ mitigar
De detección				Evitar/ eliminar
Reactivas/ correctivas				Aceptar/ asumir

Nota: Esta tabla muestra los indicadores para la correcta Gestión del Riesgo para los Derechos y Libertades que establece la Guía de la Agencia Española de Protección de Datos

Una medida técnica u organizativa o una garantía puede ser cualquier cosa desde la aplicación de soluciones técnicas avanzadas hasta la formación básica del personal. Por ejemplo que pueden ser adecuados, en función del contexto y de los riesgos asociados al tratamiento en cuestión, son la seudonimización de los datos personales; conservar los datos personales disponibles en un formato estructurado, de uso común y lectura mecánica; permitir que los interesados intervengan en el tratamiento; facilitar información acerca de la conservación de datos personales; disponer de sistemas de detección de programas maliciosos; formar a los empleados en prácticas básicas de «ciberhigiene»; establecer sistemas de gestión de la privacidad y la seguridad de la información; obligar contractualmente a los encargados del tratamiento a adoptar prácticas específicas de minimización de datos, etcétera. (Directrices 4/2019 relativas al artículo 25 Protección de datos desde el diseño y por defecto Versión 2, 2020)

De lo antes descrito, la Dirección Nacional de Tecnologías de la Información y Comunicación cumple su trabajo en el campo de la seguridad de la información y por tanto, podría implementar sistemas de gestión de la privacidad cumpliendo con la norma ISO/IEC 27701 como medida de mitigación al riesgo y evolución de impacto, además de gestionar los errores técnicos para lo cual se podría implementar: sistemas de decisión automática, sistemas de ayuda a la decisión, tratamiento biométrico, errores en la sincronización de sistemas transaccionales. (Gestión del riesgo y Evaluación de impacto en tratamientos de Datos personales, 2021).

Por otro lado, cabe mencionar que para realizar el tratamiento en datos personales (su análisis del riesgo y evaluación de impacto) se debe tomar en cuenta, también, los criterios de idoneidad, necesidad y proporcionalidad establecidos en la Guía de Gestión de Riesgos y Evaluación de Impacto de la Agencia Española de Protección de Datos con el fin de que los

derechos y libertades individuales sean el factor primordial al momento de realizar el tratamiento, así se pondera la manera en la que se realiza el tratamiento y se busca establecer lo más idóneo, lo que sea necesario y lo que sea proporcional a lo que se persigue en el tratamiento. Estos criterios consisten en:

- **Idoneidad:** Determinar si el tratamiento para los datos es el adecuado según la finalidad que se busca perseguir
- **Necesidad:** Determinar si la finalidad que se persigue puede o no alcanzarse de algún otro modo que sea menos lesivo o invasivo.
- **Proporcionalidad en sentido estricto:** Establecer que la gravedad del riesgo del tratamiento tanto para los derechos como para las libertades, e incluso la intromisión en la privacidad, debe ser la adecuada según el fin que se persigue y esta gravedad, además, debe estar proporcionada a la urgencia de esta.

3.6. Identificación de si la vulneración de la seguridad debe o no ser notificada a la autoridad de protección. Y cuáles son las formas de Notificación.

3.6.1. Resultados

3.6.1.1. Respuesta a los objetivos específicos a partir del análisis de documentos

- Examinar cuándo debe la Dirección Nacional de Tecnologías de la Información y Comunicación de la Policía Nacional del Ecuador, notificar la vulneración de la seguridad de datos personales

La Dirección Nacional de Tecnologías de la Información y Comunicación de la Policía Nacional del Ecuador debe notificar la vulneración de la seguridad de datos personales cuando conozca que existe un riesgo, amenaza o vulnerabilidad según los conceptos establecidos en la normativa ISO/IEC y la Ley Orgánica de Protección de Datos Personales, también, mencionan

ambas normas, que se debe notificar a la autoridad encargada cuando haya existido una vulneración a la seguridad de datos personales, sin embargo, debe entenderse que podría existir un escenario en donde se corra el riesgo de vulnerar los derechos fundamentales y libertades individuales con la notificación que realiza la Policía Nacional, además de ello puede vulnerar la misión que realiza esta institución cuando se conozcan estos datos sensibles y dar paso a la vulneración en la seguridad Estatal.

- Advertir cómo debe actuar la Dirección Nacional de Tecnologías de la Información y Comunicación de la Policía Nacional del Ecuador si ha existido una vulneración de la seguridad de datos personales

Existe un procedimiento adecuado para la actuación general que se da en la Policía Nacional del Ecuador, en primer lugar y de manera interna, la Dirección Nacional de Tecnologías de la Información y Comunicación de la Policía Nacional debe conocer de esta vulnerabilidad y enviar una notificación a la Comandancia General de la Policía Nacional para que esta emita la debida notificación a instancias externas y al Oficial de Seguridad de la Información elegido por el respectivo comité que debe integrar la Institución de la Policía Nacional. Esta vulneración de la seguridad datos debe ser notificada también a la Autoridad de Protección de Datos Personales y la Agencia de Regulación y Control de las Telecomunicaciones que previamente debió ser conocido por el responsable del tratamiento de datos.

- Identificar cual es el riesgo de inobservar la protección de datos personales de los servidores policiales de la Institución

El riesgo que corren los servidores policiales si no se protegen adecuadamente sus datos con tecnologías de punta es que estos queden expuestos a riesgos, amenazas y vulnerabilidades

cuando escenarios en los que, probablemente, terceros pudieran acceder a ellos con la intención de vulnerar sus derechos protegidos o libertades individuales.

3.6.1.2. Respuesta al objetivo general a partir del análisis de documentos

Así, luego de haber respondido las preguntas específicas se debe responder a la pregunta general de si La Dirección Nacional de Tecnologías de la Información y Comunicación, de la Policía Nacional del Ecuador, ¿debe (o no) notificar la vulneración de la seguridad de datos personales que constituyan un riesgo para los servidores policiales Directivo y Técnico Operativos de esta Institución? Y la respuesta que cabe es que: no se debe notificar pues esta, notificación, se realiza con datos que están regulados por la ley, sin embargo, y como se ha mencionado reiteradas veces, si existiera una vulneración a los datos personales de los servidores policiales (datos manejados por la Dirección Nacional de Tecnologías y Comunicaciones de la Policía Nacional) se conocería el estado en el que se encuentran, toda su información personal y laboral como sus asignaciones, su cargo y rango, su dirección, la misión en la que se encuentra ubicado y muchos más datos que comprometerían el trabajo que realiza la institución y por tanto la misión que debe cumplir (la de la seguridad ciudadana y orden público) pero, además, pueden resultar en vulneraciones a los derechos y libertades pues pueden quedar expuestos ante bandas delictivas que pueden usar los datos para incurrir en vulneraciones y perjuicios a su persona. Así, se entiende que estos datos personales se incluirían en el literal e del ámbito de exclusión de los datos (artículo 2 de la Ley Orgánica de Protección de Datos) por ser relevantes para la seguridad del Estado y con ello se entendería que no habría un deber de notificación en caso de que exista una vulneración a la seguridad de estos datos personales, sino que se debería buscar una alternativa a los mismos (una guía) en donde se tome en cuenta los estándares internacionales de derechos humanos, los principios de la Ley Orgánica de Protección de Datos y los criterios de proporcionalidad, legalidad

y necesidad tal como lo mencionan el artículo 2 y 11 de la Ley Orgánica de Protección de Datos para así poder proteger la seguridad de los servidores policiales y seguridad ciudadana que ellos brindan.

3.6.2. Formas de notificación

Ley Orgánica de Protección de Datos

La Ley Orgánica de Protección de Datos menciona en su artículo 43 cuál es el protocolo para realizar la notificación de la vulneración de la seguridad de datos personales si es que esto llegara a ocurrir. Dice:

> El responsable del tratamiento deberá notificar la vulneración de la seguridad de datos personales a la Autoridad de Protección de Datos Personales y la Agencia de Regulación y Control de las Telecomunicaciones, tan pronto sea posible, y a más tardar en el término de cinco (5) días después de que haya tenido constancia de ella, a menos que sea improbable que dicha violación de la seguridad constituya un riesgo para los derechos y las libertades de las personas físicas. Si la notificación a la Autoridad de Protección de Datos no tiene lugar en el término de cinco (5) días, deberá ir acompañada de indicación de los motivos de la dilación. (Ley Orgánica de Protección de Datos, 2021)
>
> El encargado del tratamiento deberá notificar al responsable cualquier vulneración de la seguridad de datos personales tan pronto sea posible, y a más tardar dentro del término de dos (2) días contados a partir de la fecha en la que tenga conocimiento de ella. (Ley Orgánica de Protección de Datos, 2021)

Guía de Gestión de Riesgo y Evaluación de Impacto de la Agencia Española de Protección de Datos

La Guía de Riesgos y Evaluación de Impacto de la Agencia Española de Protección de Datos establece, en caso de existir una vulneración de la seguridad de los datos personales, lo siguiente:

Primero, que el artículo 33.5 del Reglamento General de Protección de Datos (RGPD) establece la obligación del responsable de tratamiento de datos para documentar cualquier brecha, sus efectos y las medidas correctivas adoptadas. Así, el artículo 33 del RGPD, menciona que tan pronto como el responsable del tratamiento tenga conocimiento de que se ha dado una brecha de datos personales debe realizar la notificación a la Autoridad de Control competente, pero cuando sea probable que esta brecha configure un riesgo para los derechos y libertades de las personas. Menciona pues, que debe realizarse sin demoras o dilaciones y en un máximo de 72 horas siguientes, contando también las horas de fines de semana y festivos. Este plazo de 72 horas se comienza a calcular desde el instante en que el responsable de tratamiento constate que el incidente de seguridad ha afectado a datos personales.

La "brecha de datos personales" según el Reglamento General de Protección de Datos (2016) se determina como: "toda violación de la seguridad que ocasionen 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." Existen pues, factores determinantes para evaluar el riesgo de la brecha y se establecen en la siguiente tabla.

Tabla 4

Factores para evaluar el riesgo de una brecha

Factores para evaluar el riesgo de una brecha
• Tipo de brecha de datos personales
• Naturaleza, carácter sensible y el volumen de datos personales
• Facilidad de identificación de las personas
• Gravedad de las consecuencias para los derechos y libertades de las personas
• Características particulares del responsable de tratamiento

• Número de personas afectadas
• Consideraciones generales

Nota: Esta tabla muestra los factores que utiliza la Guía de la Agencia Española de Protección de Datos para evaluar el riesgo de una brecha de datos personales.

Ahora bien, si la brecha es detectada por el encargado del tratamiento, se entiende que éste deberá remitir al responsable toda la información necesaria para que pueda cumplir con sus obligaciones. El responsable tiene que documentar la brecha y evaluar la necesidad de notificar ante la Autoridad de Control como la necesidad de comunicar lo ocurrido a los afectados. Hay que tomar en cuenta que el encargado podrá realizar la notificación de la brecha a nombre del responsable cuando así lo conste estipulado en un contrato o vínculo legal.

Por otro lado, cuando la brecha signifique un alto riesgo para los derechos y libertades de las personas afectadas, aquí se debe notificar a la Autoridad de Control, comunicar a los afectados sin tardanza y con lenguaje claro y sencillo, de forma concisa y transparente.

La notificación de una brecha de datos personales a la Autoridad de Control es una obligación y un ejercicio de responsabilidad proactiva.

El artículo 33 del RGPD, además, establece que la notificación de brechas de datos personales a la Autoridad de Control deberá mínimo:

- "Describir la naturaleza de la violación de la seguridad de los datos personales, inclusive, cuando sea posible, las categorías y número aproximado de interesados afectados, y las categorías y el número aproximado de registros de datos personales afectados;"
- "Comunicar el nombre y los datos de contacto del delegado de protección de datos o de otro punto de contacto del que pueda obtenerse más información;"
- "Describir las posibles consecuencias de la violación de la seguridad de los datos personales;"

- “Describir las medidas adoptadas o propuestas por el responsable del tratamiento para poner remedio a la violación de la seguridad de los datos personales, incluyendo, si procede, las medidas adoptadas para mitigar los posibles efectos negativos.”

Tabla 5

Notificación de la brecha de datos personales

Notificación brecha de datos personales
Sobre el tratamiento y el responsable
Intencionalidad y origen
Tipología
Categorías de datos y perfil de los afectados
Consecuencias
Resumen de la brecha
Implicaciones transfronterizas
Información temporal y medios de detección
Medidas de seguridad preventivas
Acciones tomadas
Comunicación a los afectados

Nota: Esta tabla muestra lo que debe contener la Notificación de la brecha de datos personales

Normativa ISO/IEC

Las normativas ISO, son quienes regulan y otorgan protocolos que deben seguir quienes trabajan con la Organización Internacional para la Normalización (ISO) y la Comisión Electrotécnica Internacional (IEC) quienes conforman el denominado sistema especializado de normalización mundial, en donde los países miembros, organizaciones internacionales, gubernamentales y no gubernamentales participan en el desarrollo de normas internacionales que ayudan al tratamiento de la actividad técnica por el interés mutuo que se genera.

Esta normativa dice que se necesita un enfoque sistemático con la finalidad de gestionar el riesgo que puede existir en la seguridad de la información para encontrar los requisitos de la información que requiere una organización y así poder tener un sistema eficaz. La gestión del riesgo debe darse por medio de un proceso continuo que debe constar de varias etapas: en primer

lugar, se debe establecer el contexto, luego la evaluación del riesgo, el tratamiento del riesgo con recomendaciones y decisiones que sirvan para el riesgo tratado, su aceptación, la comunicación y por último su monitoreo y revisión; hay que tener en cuenta que los resultados de la valoración que se haga al riesgo serán la pieza clave para la eficacia que tenga el tratamiento que se le dé a éste.

En el proceso de gestión de riesgo en la seguridad de la información se debe comunicar a todo el personal operativo y a los directores sobre los riesgos identificados y el tratamiento que se den a estos.

Para comprender claramente el Proceso de Gestión de Riesgos de la Seguridad de la Información (SGSI) hay que saber que las etapas de este se encuentran establecidas en las siguientes;

- Planificación: Establecimiento del contexto, valoración del riesgo, desarrollo del plan de tratamiento y la aceptación del riesgo.
- Hacer: Implementación de las acciones y controles necesarios para reducir el riesgo hasta un nivel aceptable.
- Verificar: Los directores verán la necesidad de revisar las valoraciones y el tratamiento del riesgo.
- Actuar: Todas las acciones que son necesarias, incluso la aplicación adicional del proceso de gestión del riesgo en la seguridad de la información.

La normativa también menciona que para aceptar un riesgo se debe considerar criterios como factores legales, reglamentarios, sociales, humanitarios, entre otros, pero para la presente

investigación estos son los criterios que se deben tomar en cuenta pues se habla de razones que pueden afectar bienes jurídicos como la vida, la integridad y la libertad.

Por otro lado, dentro de una organización para que se dé el proceso de la gestión de riesgo se deberá desarrollar el proceso adecuado, identificar a las partes junto con sus funciones y responsabilidades, establecer las relaciones entre las partes y la organización, definir una ruta para la toma de decisiones y determinar los registros que deben ser conservados.

Para esta investigación se debe comprender la valoración, el análisis, evaluación, tratamiento, reducción, retención, comunicación y monitoreo del riesgo, mismo que puede llegar a ser un problema para los derechos fundamentales y libertades o libertades individuales

En cuanto a la valoración del riesgo en la seguridad de la información, hay que identificar los riesgos, describirlos y priorizar todos aquellos objetos relevantes para la organización; en esta etapa se realiza el análisis, la identificación, la estimación y la evaluación del riesgo.

En el análisis del riesgo se debe identificar, en primer lugar, los activos que viene a ser todo aquello que tiene un valor en la organización y que requiere de una protección y esta identificación debe llevarse a cabo con un buen nivel de detalle para que se pueda proporcionar la información suficiente para valorar el riesgo. Por otro lado, también se debe identificar las amenazas y sus orígenes pues esta puede llegar a causar graves daños a los activos (información, procesos, sistemas y la propia organización), las amenazas pueden tener un origen natural, humano, o ser accidentales o deliberadas lo que hace que sea necesario conocer este origen para saber cómo actuar. Hay que saber identificar, también, las vulnerabilidades ya que estas pueden ser explotadas por las amenazas y llegar a causar daños tanto a los activos como a la organización; estas vulnerabilidades se pueden identificar dentro de la organización, de los procesos y

procedimientos, de las rutinas de gestión, en el personal, en el ambiente físico, en la configuración del sistema de información, en el hardware, software o equipo de comunicaciones o en la dependencia de las partes externas y hay que tomar en cuenta que la vulnerabilidad por sí sola no puede causar un daño sino que es necesario que haya una amenaza para que pueda ser explotada. El siguiente paso es saber identificar las consecuencias mismas que pueden ser traducidas en pérdida de confidencialidad, integridad y disponibilidad de activos, posterior a esto se deben evaluar estas consecuencias, es decir el impacto que pueden llegar a tener en la organización y que pueda resultar en incidentes posibles o incidentes reales a la seguridad de la información.

Ahora bien, en cuanto a la evaluación del riesgo se deben comparar los niveles de riesgo con los criterios para la evaluación del mismo y sus criterios de aceptación. Posterior a esto se procede al tratamiento del riesgo en donde deben seleccionarse controles para poder reducir, retener, evitar o transferir los riesgos y también debe definirse un plan para este tratamiento. Una vez realizado el tratamiento hay que reducir el riesgo, esto se hace mediante una selección de controles para que el riesgo residual pueda ser revaluado como aceptable; posterior a esto se debe retener el riesgo dependiendo de la evaluación que ya se le ha hecho y por último se debe evitar cualquier tipo de actividad o acción que de origen nuevamente al riesgo o a algún otro riesgo particular.

Por otro lado, hay que tomar en cuenta que como actividades adicionales indispensables se debe: comunicar la información sobre el riesgo entre la persona que toma la decisión sobre esta y las demás partes involucradas, esto con la finalidad de llegar a un acuerdo sobre cómo se gestionan los riesgos; es decir, que se va a garantizar que los responsables de la implementación de la gestión del riesgo y quienes tienen derechos adquiridos puedan comprender las bases para poder tomar las

decisiones más adecuadas. Y también se debe monitorear, revisar y mejorar la gestión del riesgo según se considere conveniente y necesario.

Esquema Gubernamental de Seguridad de la Información (EGSI)

El Esquema Gubernamental de Seguridad de la Información (EGSI) menciona que las Instituciones de la Administración pública Central, Institucional y que dependen de la función ejecutiva (en el presente caso: La Policía Nacional del Ecuador) deben realizar una Evaluación de Riesgos sobre sus activos de información críticos y diseñar, además, un plan que trate estos riesgos; dando, por tanto, la pauta para entender que EGSI es relevante en la investigación ya que establece la guía que se utiliza para tratar los riesgos hacia la Seguridad de la Información que en el presente caso la información que se menciona vendrían a ser los datos personales de los servidores policiales.

El Esquema Gubernamental de Seguridad de la Información (EGSI) se centra en la organización que se crea dentro de una de las instituciones mencionadas en el párrafo anterior y que tiene que ver con la seguridad de la información, por tanto, en primer lugar menciona que la máxima autoridad de una de las instituciones nombradas va a designar un Comité de Seguridad de la Información (CSI), este Comité estará integrado por los responsables de: Talento Humano, el área Administrativa, el área de Planificación y Gestión estratégica, el de Comunicación Social, el de las Tecnologías de la Información, el de las Unidades Agregadores de Valor y el del Arca Jurídica quien participará como asesor; este comité tiene como finalidad el poder garantizar y facilitar la adecuación e implementación de iniciativas referentes a la seguridad de la información dentro de la institución a la que representan.

Hay que tener en cuenta que el Comité tiene las siguientes atribuciones relevantes: El realizar el seguimiento de los cambios significativos de los riesgos que llegasen a afectar a la información frente a amenazas, el conocer y supervisar la investigación y monitoreo de los incidentes que pudieran darse respecto a la seguridad de la información y la coordinación de la implementación de controles de la seguridad de la información para la implementación de nuevos sistemas y servicios, es decir que todos estos atributos van ligados a la normativa ISO y buscan la prevención, el control o la eliminación de los riesgos que pudiesen existir en la información y que pudieren vulnerar derechos y libertades.

Por otro lado, EGSI, dice que este Comité va a designar dentro de su respectiva institución a un funcionario que ocupará el cargo de Oficial de Seguridad de la Información (OSI) mismo que debe tener un conocimiento en la Seguridad de la Información y en la Gestión de Proyectos. El Oficial de Seguridad de la Información, dentro de los atributos más relevantes para la investigación, debe elaborar un plan de concientización para la seguridad de la información en donde abarque actividades continuas sobre esta concientización, en donde realice charlas a los nuevos funcionarios y en donde realice un plan con medidas disciplinarias en caso de violación a la seguridad de la información; por otro lado, también debe buscar generar y orientar el procedimiento adecuado para manejar aquellos incidentes detectados o reportados con respecto a la seguridad de la información y debe también, coordinar la gestión de estos incidentes a través de otras instituciones gubernamentales, es decir que el Oficial de Seguridad de la Información es una de las piezas fundamentales en caso de que exista la vulneración a los datos personales en una institución como la Policía Nacional del Ecuador y el encargado de gestionar los incidentes hacia instituciones externas que requieran de su notificación.

Otro de los puntos a tratar es el Sistema de Gestión de Seguridad de la Información (SGSI) que se menciona en este acuerdo y que viene a constituirse como el elemento más importante de la normativa ISO 27001 pues es quien unifica los criterios para la evaluación que se hace de los riesgos que están asociados al manejo de la información institucional.

Respecto a la notificación de incidentes de la seguridad de la información menciona que se debe establecer formalmente responsabilidades y procedimientos para asegurar una respuesta rápida, efectiva y acorde a los incidentes de seguridad de la información que pueden ocurrir en la institución. Y aquí establece que se debe notificar a todos los funcionarios afectados por el incidente de la restauración del equipo, sistema o servicio afectado, una vez esté solucionado el incidente. También, debe elaborar, implementar y socializar el procedimiento formal para reportar los eventos de seguridad de la información, a través de los canales respectivos. Y hay que realizar la aplicación de procedimientos establecidos, para responder ante incidentes de seguridad de la información, notificando al Oficial de Seguridad de la Información de la institución.

Además, el proceso de gestión del riesgo en la seguridad de la información se debe monitorear, revisar y mejorar continuamente, según sea necesario y adecuado y todas las mejoras acordadas para el proceso o las acciones necesarias para mejorar la conformidad con el proceso se deberían notificar al Comité de Seguridad de la Información, para tener seguridad de que no se omite ni subestima ningún riesgo o elemento del riesgo, y que se toman las acciones necesarias y las decisiones para brindar una comprensión realista del riesgo y la capacidad para responder

Por último, este acuerdo ministerial dentro de sus anexos contiene lo que es el proceso para la gestión del riesgo de la seguridad de la información, mismo que se analiza en el documento de la normativa ISO con más detalle, pero que consta de las siguientes actividades:

- Establecimiento del contexto
- Valoración del riesgo
- Tratamiento del riesgo
- Aceptación del riesgo
- Comunicación del riesgo
- Monitoreo y revisión del riesgo

3.6.3. Propuestas de alternativas de solución

Propuesta 1:

Creación de la Unidad Administrativa que tendrá a cargo las funciones de Protección de Datos Personales como sugerencia se podrá denominar Departamento de Seguridad de Protección de Datos Personales en concordancia con la Ley vigente.

Propuesta 2:

Protocolo o guía de respuesta en el caso de que exista una vulneración a la seguridad de datos personales de los servidores policiales para saber cómo deben actuar y que así no corran riesgo sus derechos fundamentales y libertades individuales. Este protocolo o guía servirá para la educación de los servidores policiales en capacitaciones sobre la protección de datos personales.

Los posibles puntos guías para la guía de solución serían:

1. Alertar la vulneración a los datos que maneja en la Dirección Nacional de Tecnologías de la Información y Comunicación de la Policía Nacional, mediante un firewall o un sistema de seguridad de la información de manera interna al departamento de Seguridad de la Información.
2. Conocer de qué tipo de datos se trata

3. No emitir una notificación a la Autoridad de protección de datos, si es que estos no están en el ámbito de aplicación de la Ley Orgánica de Protección de Datos (literal e) para no alterar la seguridad, tanto de los servidores policiales como de la seguridad estatal.
4. Ponderar los datos con los derechos y libertades individuales siguiendo los criterios de proporcionalidad, necesidad e idoneidad establecidos en la Guía de Gestión de Riesgos y Evaluación de Impacto de la Agencia Española de Protección de Datos
5. Realizar el tratamiento de los datos establecido en la Guía de Gestión de Riesgos y Evaluación de Impacto de la Agencia Española de Protección de Datos
6. Realizar el tratamiento de la Seguridad de la Información establecido en la normativa ISO /IEC 27000
7. Tomar en cuenta los principios establecidos en la Ley Orgánica de Protección de Datos a lo largo de todo el tratamiento
8. Una vez concluido el tratamiento inmediato, establecer los resultados positivos para la prevención del ataque reiterado de la misma amenaza y de amenazas futuras.
9. Notificar a la autoridad de protección de datos acerca de lo sucedido para que pueda registrarlo, informando que los datos son confidenciales y sensibles y que por tanto necesitaban este tratamiento excepcional y de la no notificación inicial a la Autoridad de Protección de Datos pues no entran en su ámbito de aplicación.

Propuesta 3:

Según la Disposición Transitoria Segunda de la Ley Orgánica de Protección de Datos (2021): "Todo tratamiento realizado previo a la entrada de esta ley deberá adecuarse a lo previsto en ella dentro del plazo de dos años contados a partir de su publicación en el Registro Oficial. El incumplimiento a esta disposición dará lugar a la aplicación del régimen sancionatorio establecido

en esta Ley". Por tanto, como propuesta a este régimen sancionatorio se debe revisar las infracciones dentro del Código Orgánico de Entidades de Seguridad Ciudadana y Orden Público establecido en el Título Tercero del Régimen Administrativo Disciplinario y revisar el Estatuto Orgánico de Gestión Organizacional por Procesos de la Policía Nacional para poder incluir las sanciones por el no actuar adecuado en caso de una vulneración a la seguridad de los datos.

3.7. Justificación Y Aplicación De La Metodología

3.7.1. Nivel de estudio

La presente investigación constituye un nivel de estudio tanto exploratorio como descriptivo; exploratorio porque se busca examinar un tema poco estudiado como es conocer si la Policía Nacional del Ecuador debe notificar la vulneración de la seguridad de datos personales de los servidores policiales a la Autoridad de Protección de Datos Personales y la Agencia de Regulación y Control de las Telecomunicaciones; y, descriptivo porque se busca identificar los diversos aspectos y circunstancias de la obligación jurídica que tendría la Policía Nacional del Ecuador en este campo.

3.7.2. Modalidad Investigación

La modalidad de investigación que se empleará es la documental y la de proyecto de desarrollo. La modalidad documental porque se busca ampliar y profundizar el conocimiento con apoyo de documentos y registros (doctrina, normativa, jurisprudencia, sistemas informáticos o bases de datos), esquema gubernamental de seguridad de la información y estándares con reconocimiento internacional. Por otro lado, la modalidad del proyecto de desarrollo se utiliza al encaminar la investigación hacia una temática basada en una necesidad existente en la Policía Nacional del Ecuador para cumplir las disposiciones contenidas en la Ley Orgánica de Protección de Datos Personales expedida en el año 2021.

3.7.3. Métodos

La presente investigación usará dos métodos: El inductivo-deductivo y el analítico-sintético. El inductivo-deductivo pues a partir de un concepto general como es la Protección de Datos en el Ecuador se lleva a la aplicación en un contexto más específico como es el caso de la notificación de la vulneración de la seguridad de datos personales hacia los servidores policiales; una vez resuelta esta problemática d, se espera contribuir al conocimiento general de la Protección de Datos en el Ecuador. Por otro lado, se usará el método analítico-sintético porque se busca hallar todo lo que comprende el Sistema de Protección de Datos (el cómo funciona, sus principios, sus relaciones, sus conceptos básicos y secundarios, etc.) y posteriormente se pretende recomponer estos datos para conocer de manera progresiva y sistemática cómo funciona todo el aparataje en caso de que se produzca una vulneración de la seguridad de datos personales y el actuar de la Policía Nacional del Ecuador.

3.7.4. Población y muestra

No es necesario hacer el cálculo de población y muestra ya que es un estudio netamente cualitativo que no exige el uso del cálculo de una muestra

3.7.5. Instrumentos de investigación

El instrumento de investigación, que tiene como finalidad esencial el recoger la información que posteriormente se convertirán en resultados relevantes, será el análisis de documentos pues se busca estudiar varios documentos y registros (doctrina, normativa, jurisprudencia, sistemas informáticos o bases de datos) que se refieren a la protección de datos personales, así como también los procedimientos que debe seguir la Policía Nacional del Ecuador para notificar las vulneraciones de la seguridad de datos personales que pudieran darse a los servidores policiales.

3.7.6. Procesamiento de datos

El procesamiento de datos de la presente investigación va a tener como base el uso de Microsoft Office en el cual el manejo de todos los textos se hará a través de Word, por otro lado, el registro de datos a través de gráficos se realizará en Excel y la presentación final se realizará en Power Point. Para la gestión de referencias bibliográficas se utilizará Zotero y para detectar y prevenir el plagio se usará el software Ouriginal de Turnitin.

.3.7.7. Protocolos de investigación

Tabla 6

Protocolo de Investigación

OBJETIVOS ESPECÍFICOS	PROTOCOLO
Examinar cuándo debe la Policía Nacional del Ecuador, notificar la vulneración de la seguridad de datos personales	• Conocer sobre casos internacionales donde haya existido vulneración a la seguridad de datos personales • Conocer la normativa, doctrina, jurisprudencia, sistemas informáticos o bases de datos que rige la protección de los datos personales • Realizar una comparación entre la normativa de protección de datos personales y los casos identificados para establecer cuándo debe notificarse por parte de la Policía Nacional del Ecuador la vulneración de la seguridad de datos personales a sus servidores policiales
Advertir cómo debe actuar la Policía Nacional del Ecuador si ha existido una vulneración de la seguridad de datos personales	• Conocer cómo funciona y cuál es el actuar de la Dirección Nacional de las Tecnologías de la Información y comunicación de la Policía Nacional del Ecuador frente a casos de vulneración de la seguridad de datos personales ▪ Identificar qué tipo de vulnerabilidad ha sufrido los datos personales ▪ Notificar a la Comandancia General de la Policía Nacional del Ecuador. • Identificar casos nacionales e internacionales en donde haya existido vulneración de la seguridad de datos personales • Conocer sobre la normativa que rige la protección de estos datos personales
Identificar cual es el riesgo de inobservar la protección de datos personales de los servidores policiales de la Institución	• Conocer cuál es la institución que se encarga de manejar los datos personales de los servidores policiales • Conocer cuál es el protocolo que se debe seguir para proteger los datos personales • Conocer cuál es el protocolo que se debe seguir en caso de que los datos personales sean vulnerados • Identificar casos nacionales o internacionales en donde la inobservancia de la protección de datos personales ha sido perjudicial • Establecer posibles escenarios perjudiciales y no perjudiciales que puedan llegar a suceder si no se protegen los datos personales • Realizar un contraste del material identificado para establecer la cantidad de riesgo que puede llegar a existir por la inobservancia de la protección de datos.

Nota: Esta tabla muestra el protocolo a seguir para conocer cada uno de los objetivos específicos

5. CONCLUSIONES

- La inversión estatal en la seguridad hacia las Tecnologías de la Información y Comunicación (TIC's) es precaria, esto genera que no exista la capacitación suficiente a los servidores que se encargan de la seguridad de datos indispensables para la seguridad estatal; genera, también, que no exista la inversión suficiente en proyectos para un cambio en la tecnología de plataformas estatales y con ello se tenga una administración ineficiente, junto con el reforzamiento inapropiado de la seguridad y la protección en ciberataques.
- La Dirección Nacional de Tecnologías de la Información y Comunicación de la Policía Nacional del Ecuador trabaja con datos personales de los servidores policiales, estos datos son de carácter sensible en cuanto pueden llegar a constituir un riesgo para el servidor policial si es que llegasen a ser hackeados, ya que las bandas delictivas pueden tomar estos datos para conocer sobre todos y cada uno de ellos e incurrir en una afectación y perjuicio hacia su persona, vulnerando así sus derechos y libertades individuales.
- La Dirección Nacional de Tecnologías de la Información y Comunicación de la Policía Nacional del Ecuador no debería tener la obligación de notificar cuando existiese una vulneración a la seguridad de datos personales de los servidores policiales (talento humano) que manejan pues La Dirección Nacional de Tecnologías de la Información y Comunicación debe notificar vulneraciones a la seguridad de datos personales cuando estos datos estén regulados en la Ley Orgánica de Protección de Datos Personales, sin embargo, los datos de los servidores policiales se encuentran excluidos de su ámbito de aplicación por cuanto pueden ser esenciales para la seguridad estatal, ya que si se conocen datos como el estado del servidor policial, sus asignaciones, misiones, cargo, etc., generaría un riesgo al trabajo de la institución policial; dando paso a que su misión, también, se comprometa

(seguridad ciudadana y orden público); generando, a su vez un riesgo y perjuicio a la seguridad del Estado.

6. RECOMENDACIONES

- Implementación de una unidad administrativa de protección de datos
- Generar la dotación de recursos humanos financieros y logísticos, técnicamente de la más alta calidad a la Dirección Nacional de Tecnologías de la Información y Comunicación
- Implementación de programas de capacitación anual a los servidores policiales que formen parte de la Dirección Nacional de Tecnologías de la Información y Comunicación
- Reforma al Título Tercero del Régimen Administrativo Disciplinario del Código Orgánico de Entidades de Seguridad Ciudadana y Orden Público para establecer un régimen disciplinario en donde se establezca la sanción en caso de que no se genere la alerta cuando existe la vulneración de la seguridad de datos.

7. REFERENCIAS

AEPD. (s.f.). Notificación de brechas de datos personales (art. 33 RGPD). https://sedeagpd.gob.es/sede-electronica-web/vistas/infoSede/nbs/guiadoBrechasInicio.jsf

Agencia Española de Protección de Datos. (2021). Gestión del riesgo y evaluación de impacto en tratamientos de datos personales. https://www.aepd.es/sites/default/files/2019-09/guia-evaluaciones-de-impacto-rgpd.pdf

Álvarez, M., Escobar, A. (2022). Análisis de ciberataques sobre el uso de redes sociales en relación a la protección de datos personales en Ecuador. Dom. Cien., ISSN: 2477-8818 Vol. 8, núm. 1. Febrero Especial, 2022, pp. 1070-1079. DOI: http://dx.doi.org/10.23857/dc.v8i1.2622

Banco Central del Ecuador. (2022). ECUADOR REGISTRÓ UN CRECIMIENTO INTERANUAL DE 3,8% EN EL PRIMER TRIMESTRE DE 2022.

https://www.bce.fin.ec/index.php/boletines-de-prensa-archivo/item/1514-ecuador-registro-un-crecimiento-interanual-de-3-8-en-el-primer-trimestre-de-2022

Benavides, C., Benavides, J., Santillán, A. (2021). Principios que rigen el uso progresivo de la fuerza y su aplicación en la Policía Nacional. *Dilemas contemporáneos: educación, política y valores*, *8*(spe3), 00024. Epub 30 de agosto de 2021. https://www.scielo.org.mx/scielo.php?pid=S2007-78902021000500024&script=sci_arttext

Brian Nougrères, Ana. - "De la protección de datos personales y la cooperación internacional", en Anuario de Derecho Informático Nº VI. Montevideo, 2006.

Cárdenas, J. (2014). Noción, justificación y críticas al principio de proporcionalidad. *Boletín mexicano de derecho comparado*, *47*(139), 65-100. https://www.scielo.org.mx/scielo.php?script=sci_arttext&pid=S0041-86332014000100003#:~:text=El%20subprincipio%20de%20idoneidad%20consta,perseguir%20el%20fin%20constitucionalmente%20leg%C3%ADtimo.

Carrera, M. (2019). EL CAMBIO DE LAS POLÍTICAS DE SEGURIDAD INFORMÁTICA OCURRIDAS POR LA CREACIÓN DE NUEVAS INSTITUCIONES A PARTIR DEL AÑO 2013 EN EL ECUADOR. [Tesis de Titulación, Universidad de las Américas]. https://dspace.udla.edu.ec/bitstream/33000/11169/1/UDLA-EC-TLCP-2019-37.pdf

Casas, C. (2019). ¿Qué son los estándares de Derechos Humanos? Revista Internacional de Derechos Humanos / ISSN 2250-5210 / 2019 Vol. 9, No. 2 revistaidh.org. https://perso.unifr.ch/derechopenal/assets/files/articulos/a_20200608_04.pdf

Cedeño, R. (2021). Ciberseguridad y Ciberdefensa: Perspectiva de la situación actual en el Ecuador. Revista Tecnológica Ciencia y Educación Edwards Deming. ISSN: 2600-5867.

Enero-Marzo Vol6. -1- 2022. https://revista-edwardsdeming.com/index.php/es/article/view/88/158

Cobarrubias, P. (2013). Estándares Internacionales de Seguridad Informática. https://es.slideshare.net/PedroCobarrubias/seguridad-informtica-26154937

Código Orgánico De Las Entidades De Seguridad Ciudadana Y Orden Público, 2017.

Collaguazo, J. (2020). Informe de Evaluación de Riesgos. Implementación de un sistema de Gestión de Seguridad de la Información (SGSI) para la Policía Nacional del Ecuador.

Comisión Europea. (s.f.). ¿Qué son los datos personales? https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-personal-data_es

Comisión Interamericana de Derechos Humanos. ´ (2009). INFORME SOBRE SEGURIDAD CIUDADANA Y DERECHOS HUMANOS. HTTPS://WWW.CIDH.OAS.ORG/COUNTRYREP/SEGURIDAD/SEGURIDADVII.SP.HTM

Computer Hoy. (2014). ¿Qué es el cifrado de datos y cómo funciona? https://computerhoy.com/noticias/software/que-es-cifrado-datos-como-funciona-14523

Condé, H. Victor. 1999. A Handbook of International Human Rights Terminology (2nd ed. Lincoln: University of Nabraska Press.

Corte Constitucional del Ecuador. (2022). Dictamen No. 4-22-RC/22. CASO No. 4-22-RC.

Dávila, J., Godoy, E. (2020). Prospectiva de la seguridad ciudadana y su incidencia en la seguridad nacional, al año 2035. [Tesis de Maestría, Universidad de las Fuerzas Armadas]. http://repositorio.espe.edu.ec/bitstream/21000/23901/1/T-ESPE-044338.pdf

Declaración Universal de los Derechos Humanos, 1948

Diccionario Prehispánico del Español Jurídico. (2022). Ámbito de aplicación. https://dpej.rae.es/lema/%C3%A1mbito-de-aplicaci%C3%B3n#:~:text=Territorio%20al%20que%20se%20aplica%20una%20norma%20jur%C3%ADdica.

Dictamen No. 001-14-DRC-CC de 31 de octubre de 2014 (caso No. 1-14-RC).

DIRECCIÓN NACIONAL DE PLANIFICACIÓN Y GESTIÓN ESTRATÉGICA. (2022). Plan Estratégico con Visión Prospectiva de la Policía Nacional 2021 – 2025. https://www.policia.gob.ec/wp-content/uploads/downloads/2022/09/Plan-Estrategico-2025_compressed.pdf

Dirección Nacional de Tecnologías de la Información y Comunicaciones. (2021). Policía Nacional del Ecuador. Recuperado de https://www.policia.gob.ec/direccion-nacional-de-tecnologias-de-la-informacion-y-comunicaciones/

DIRECCIÓN NACIONAL DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN. (2021). RENDICIÓN DE CUENTAS 2021. https://www.policia.gob.ec/wp-content/uploads/downloads/2022/04/Presentacion-RC-2021_-final.pdf

ENTORNO ECONÓMICO. (2012). Órgano de Examen de las Políticas Comerciales - Examen de las políticas comerciales - Informe de la Secretaría - Ecuador – Revisión. WT/TPR/S/254/Rev.1 https://docs.wto.org/dol2fe/Pages/SS/directdoc.aspx?filename=S:/WT/TPR/S254R1-02.pdf&Open=True

ESTATUTO ORGÁNICO DE GESTIÓN ORGANIZACIONAL POR PROCESOS DE LA POL ICÍA NACIONAL, 2019.

González Monguí, P.E. (2017). Delitos contra la libertad individual y otras garantías. Editorial Universidad Católica de Colombia. Colección JUS Penal, No. 17.

Gonzalez, J. (2011). ¿Seguridad Informática o Seguridad de la Información? http://www.seguridadparatodos.es/2011/10/seguridad-informatica-o-seguridad-de-la.html

Guía para la Notificación de Brechas de Datos Personales de la Agencia Española de Protección de Datos, 2021

Guillermo Cabanellas de Torre. (2006). Diccionario Jurídico Elemental. https://unidaddegenerosgg.edomex.gob.mx/sites/unidaddegenerosgg.edomex.gob.mx/files/files/Biblioteca%202022/G%C3%A9nero%2C%20Sociedad%20y%20Justicia/GSJ-11%20Diccionario%20juri%CC%81dico%20elemental.%20Guillermo%20Cabanellas%20de%20Torres.pdf

Guzmán, J.M. (s.f.). El derecho a la integridad personal. CINTRAS. http://www.cintras.org/textos/congresodh/elderechoalaintegridadjmg.pdf

IBM. (s.f.). ¿Qué es el cifrado? Definición de cifrado de datos. https://www.ibm.com/es-es/topics/encryption

ISO Tools Excellence. (s.f.). ISO 27001 https://www.isotools.org/normas/riesgos-y-seguridad/iso-27001/

ISO. (s.f.). Norma ISO 25237:2017 Informática de la salud: seudonimización. https://www-iso-org.translate.goog/standard/63553.html?_x_tr_sl=en&_x_tr_tl=es&_x_tr_hl=es-419&_x_tr_pto=sc

Kaspersky. (s.f). ¿Qué es el cifrado de datos? Definición y explicación. https://latam.kaspersky.com/resource-center/definitions/encryption

Ley Orgánica De Protección De Datos Personales, 2021.

Mayer Lux, Laura. (2017). EL BIEN JURÍDICO PROTEGIDO EN LOS DELITOS INFORMÁTICOS. Revista chilena de derecho, 44(1), 261-285. https://www.scielo.cl/scielo.php?pid=S0718-34372017000100011&script=sci_arttext&tlng=pt

Morán, C. (2017). SEGURIDAD INFORMÁTICA Y REALIDAD JURÍDICA DEL CIBERESPACIO EN EL ECUADOR. [Tesis de Titulación, Universidad de las Américas]. https://dspace.udla.edu.ec/bitstream/33000/7974/3/UDLA-EC-TAB-2017-70.pdf

Naciones Unidas. (2022). Normas Internacionales. https://www.ohchr.org/es/special-procedures/sr-freedom-of-assembly-and-association/international-standards-rights-freedom-peaceful-assembly-and-association

Nahabetián Brunet, L. (2020). DERECHOS FUNDAMENTALES PARA EL GOBIERNO DE LA INFORMACIÓN: PROTECCIÓN DE DATOS PERSONALES ACCESO A LA INFORMACIÓN PÚBLICA SEGURIDAD DE LA INFORMACIÓN. Prudents Data.

Oxfam Intermón. (2020). Los derechos fundamentales: ¿cuáles son?.https://blog.oxfamintermon.org/derechos-fundamentales-cuales-son/

Pérez, J. (2016). Protección de datos y seguridad de la información. https://www-digitaliapublishing-com.bibliotecavirtual.udla.edu.ec/visorreadspeaker/110009

Policía Nacional del Ecuador. (2021). Política General de Seguridad de la Información de la Policía Nacional del Ecuador.

Rallo Lombarte, A. (2019). El nuevo derecho de protección de datos. Revista Española de Derecho Constitucional, 116, 45-74. doi: https://doi.org/10.18042/cepc/redc.116.02

Real Academia Española. (2022). Juicio. Diccionario de la Lengua Española. https://dle.rae.es/juicio?m=form

Registro Oficial. (2021). PROFORMA DEL PRESUPUESTO GENERAL DEL ESTADO CORRESPONDIENTE AL EJERCICIO ECONÓMICO 2022 Y LA PROGRAMACIÓN PRESUPUESTARIA CUATRIANUAL 2022- 2025. https://www.finanzas.gob.ec/wp-content/uploads/downloads/2021/12/REGISTRO-OFICIAL-Segundo-Suplemento-No-599-PYF-2022-Y-PCC-2022-2025_.pdf

Sain, M. (2009). La reforma policial en América Latina Una mirada crítica desde el progresismo. Nueva Sociedad.

Sosa Sacio, J.M. (2018). La libertad constitucional. Tres modelos esenciales de libertad y tres derechos de libertad. Pensamiento Constitucional N° 23, 2018 / ISSN 1027-6769.

Teodorico, T. (2020). El principio de legalidad como exigencia mínima de legitimación del poder penal del Estado.Revista Oficial del Poder Judicial, 12 (14): 249-266. https://revistas.pj.gob.pe/revista/index.php/ropj/article/view/267/412

8. ANEXOS

Tabla 7

Algunos módulos del Sistema SIIPNE publicados en Rendición de cuentas 2015

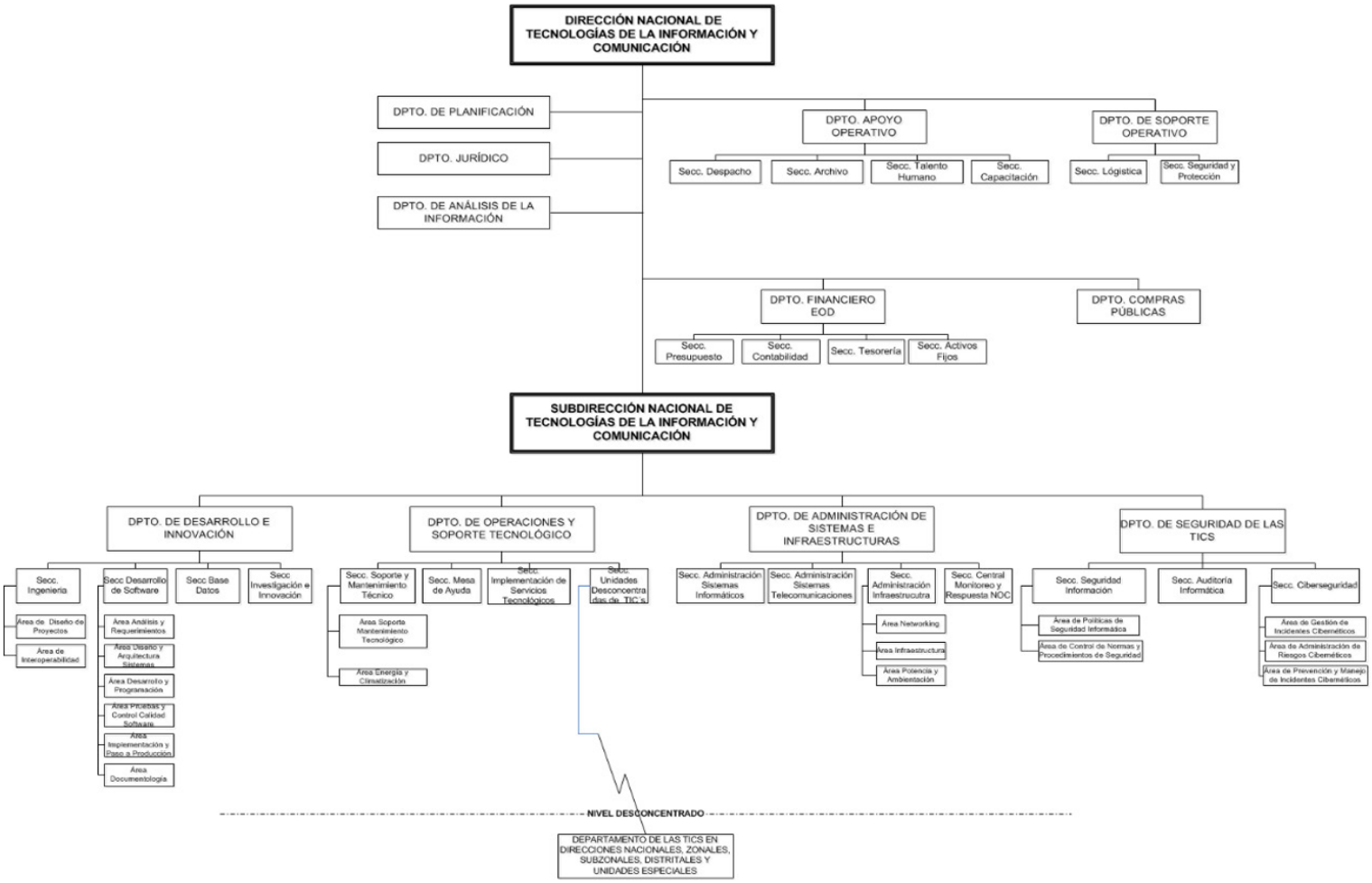
SIIPNE	
CONEXIÓN INTERPOL	Funcionando Interpol y Migración a nivel de Puertos y Aeropuertos
DESARROLLO DEL PARTE POLICIAL WEB	Implementación Ministerio del Interior
DESARROLLO DEL MÓDULO DE LOGÍSTICA	Funcionando a nivel nacional
INTERCONEXIÓN CON EL REGISTRO CIVIL	Ingreso al sistema de investigaciones
DESARROLLO DEL SISTEMA «CERO PAPELES» DOCPOL	Funcionando DNPJ, DNE, DGO
INTERCONEXIÓN Y WEB SERVICES CON LA ANT	Consulta en módulo investigaciones
INTERCONEXIÓN DINARDAP	Migración – Policía – Otras Instituciones

POLICIA NACIONAL DEL ECUADOR

Nota: Esta tabla muestra algunos módulos del sistema SIIPNE de la Dirección Nacional de Tecnología de la Información y Comunicación

Figura 1

Estructura de la Dirección Nacional de tecnología de la Información y Comunicación



Nota: La figura representa la estructura de la Dirección Nacional de Tecnologías de la Información y Comunicación.