UNIVERSIDAD PERUANA DE LAS AMÉRICAS

ESCUELA PROFESIONAL DE DERECHO

TRABAJO DE INVESTIGACIÓN

ANÁLISIS DEL ACUERDO DE CONFIDENCIALIDAD EN LA DIRTIC DE LA POLICÍA NACIONAL DEL PERÚ, 2021

PARA OPTAR EL TÍTULO PROFESIONAL DE ABOGADO

AUTOR:

VALENZUELA NEYRA MARILYN DEL CARMEN
CÓDIGO ORCID: 0000-0001-5157-5152

ASESOR: Mg.

SIALER NIQUEN CARLOS ALBERTO
CÓDIGO ORCID: 0000-0003-2965-3497

LÍNEA DE INVESTIGACIÓN: DERECHO PENAL, CIVIL Y CORPORATIVO

LIMA, PERÚ

FEBRERO, 2022

RESUMEN

El trabajo titulado “Análisis del acuerdo de confidencialidad en la DIRTIC de la Policía Nacional del Perú, 2021”, tuvo como objetivo, analizar acerca del acuerdo de confidencialidad en la DIRTIC de la Policía Nacional del Perú, 2021.

Asimismo, abarcó el acuerdo de confidencialidad donde se protege acerca de los datos de información de manera personal de cada de uno de los individuos, que tiene respaldo con relación a la Ley N° 29733, para garantizar seguridad y protección, para que no se infringe los derechos de la persona, también abarca la mencionada ley los principios rectores, para el respaldo de la protección de datos.

Además, en el estudio de la variable se empleó Leyes, Normativas, antecedentes de trabajo y artículo, los cuales permitieron ampliar la información del trabajo y se declara con exactitud sobre el acuerdo de confidencialidad. Por otro lado, también en el estudio se desarrolló las conclusiones y recomendaciones, las cuales fueron dirigidas mediante la información recolectada durante el desarrollo del trabajo.

Palabras clave: Confidencialidad, principios rectores, protección de datos personales.

ABSTRACT

The work entitled "Analysis of the confidentiality agreement in the DIRTIC of the National Police of Peru, 2021", had the objective of analyzing the confidentiality agreement in the DIRTIC of the National Police of Peru, 2021.

It also covered the confidentiality agreement which protects the personal information data of each of the individuals, which is supported in relation to Law No. 29733, to ensure security and protection, so that the rights of the person are not infringed, also covers the aforementioned law the guiding principles for the support of data protection.

In addition, in the study of the variable was used Laws, Regulations, work background and article, which allowed to expand the information of the work and it is accurately stated about the confidentiality agreement. On the other hand, the study also developed conclusions and recommendations, which were addressed through the information collected during the development of the work.

Key words: Confidentiality, guiding principles, personal data protection.

TABLA DE CONTENIDOS

I. INTRODUCCIÓN

En nuestro Estado peruano los datos de información personales son la identificación de una persona natural, de tal manera que esto se encuentra regulado en la Ley N° 29733 que tiene como objetivo garantizar acerca de la protección de datos personales, asimismo está señalado en nuestra carta magna en su artículo 2, numeral 6 donde respalda que los servicios informáticos tanto públicos como privados no deberán suministrar información que afecte la intimidad ya sea personal o familiar (Congreso de la República, 2011).

Asimismo, en el Perú, con relación a los datos de información, se presentan varios contratos, destacándose más los contratos de trabajo, donde el empleador realiza un contrato con la persona que será su trabajador; ambas partes firman y con ello se constituye deberes, derechos y obligaciones que ambas partes deben de cumplir (Jaramillo & Campos, 2019).

Por ello, lo mencionado anterior, es muy importante que se señale también el acuerdo de confidencialidad, ya que es la manifestación de voluntad de dos personas con la obligación de poder guardar y, asimismo, no revelar a terceras personas acerca de la información que uno de los sujetos desea proteger y asegurar a que no se divulgue ninguna información (Buelvas Fattoni, 2017).

En Colombia, en referencia con la protección de datos personales, se tiene la normativa que es la Ley 1581 de 2012, la cual presenta como objetivo desarrollar acerca del derecho constitucional que tienen todas las personas en poder conocer, actualizar y rectificar acerca de las informaciones que se hayan almacenado en las bases de datos o en los archivos, ante ello se presenta 8 principios para la protección de datos, de acuerdo a su artículo 4, literal h, que hace mención el principio de confidencialidad, que detalla acerca que todas las personas que tengan tratamiento de sus datos personales, y estas no

tengan la naturaleza de púbicos están completamente obligadas a poder garantizar su reserva de información (Congreso de Colombia, 2012).

Por otro lado, en Ecuador se promulgó la primera Ley Orgánica de Protección de datos Personales, la cual tiene como finalidad garantizar el ejercicio acerca del derecho a la protección de datos personales, por ello, se incluye el acceso y decisión para que la información y los datos, sean protegidos con el respaldo de los principios, derechos, obligaciones y mecanismos que lo tutelan. Por ello, en su artículo 10 de la mencionada ley precisa acerca de 13 principios donde la que se destaca más en el principio de confidencialidad, ya que la información no debe tratarse para un fin distinto la cual ya fueron recogidos por ello es sigilo y secreto o al menos que se presenten causales de supuesto tratamiento legítimo de datos personales que está consagrado en el artículo 7 de misma norma legal (República de Ecuador, 2021).

Por consiguiente, el trabajo tiene como objetivo de estudio, realizar un análisis acerca del acuerdo de confidencialidad en la DIRTIC de la Policía Nacional del Perú, 2021.

Asimismo, se abarcó en el presente estudió el desarrollo acerca de investigaciones tanto de nivel nacional como inter nacional, por consiguiente, se realizó las bases teóricas relacionadas con el tema del estudio esto de acuerdo con doctrinas, normas jurídicas, leyes, jurisprudencias, tratados para de esta manera llegar a las conclusiones. Asimismo, se detalló el aporte a la investigación con respecto a la confidencialidad que está relacionada con la protección de datos personales y, por último, se mencionaron las recomendaciones del tema en investigación.

II. ANTECEDENTES

2.1. NACIONALES

Niño Morante (2019) en su tesis detalló en su objetivo general, modelar un sistema para la seguridad de información para reforzar la confidencialidad, integridad, disponibilidad y monitorear la información de los procesos claves que se ubican en la gerencia del Instituto Nacional de Estadística e Informática- INEI de Lambayeque. La metodología que empleó fue de tipo transversal, descriptiva, por lo que contó con una población y muestra de 37 trabajadores de ODEI de Lambayeque pertenecientes a diversas áreas pertenecientes a la administración del INEI, donde empleó un cuestionario para medir el análisis de riesgo, y una encuesta para los colaboradores. En los resultados, se evidenció que la información es accedida para solamente las personas autorizadas, donde se clasificó como alta, media y baja, y en los análisis de amenazas se observó que la pérdida o alguna manipulación de la información, afecta de manera directa a la confidencialidad e integridad acerca de los activos de información por parte de la institución, de tal modo que esto surge al no haber una adecuada política el almacenamiento y el control para la información. El autor concluyó que la norma NTP ISO/IEC 27001:2014 es una manera de solución con respecto a la ausencia de la gestión de seguridad con respecto a la información del INEI de Lambayeque ya que esto permitirá implementar un sistema de gestión para fortalecer la confidencialidad, integridad y disponibilidad con relación a los activos de información, y también reforzar el monitoreo en los procesos CORE de dicha institución.

Chávez Rodríguez (2018) en su investigación señaló en su objetivo general, determinar acerca de la influencia del delito contra datos y también los sistemas informáticos con respecto al derecho a la intimidad personal en la Corte Superior de Justicia de Lima, 2017. El método que empleó fue un enfoque cuantitativo, de tipo básico,

diseño no experimental, transversal. Por lo cual, su población estuvo representada por 510 profesionales de la carrera de derecho que laboran en dicha institución, de tal manera que su muestra fue de 220 abogados, empleó como instrumento: fichas bibliográficas, cuestionarios, guías de análisis documental. En los resultados, se evidenció que el delito contra datos y sistemas informáticos con respecto a la modalidad de confidencialidad, tuvo una influencia de nivel media, al igual que su correlación entre ambas variables. El autor detalló, a modo de conclusión, que este delito afecta un 28 % con relación al derecho fundamental que es la intimidad de la persona.

Zacarias Villafranca (2017) en su investigación tuvo como objetivo determinar la influencia de un modelo de seguridad de la información basado en la norma ISO/IEC 27001:2013 para mitigar los riesgos a los activos de información en la Central de Operaciones Policiales de la Región Policial Junín. Contó con una metodología de tipo aplicada a nivel explicativo. Se trabajó con una muestra teniendo a la totalidad del personal policial que labora en la Central de Operaciones Policiales de la Región Policial Junín. Se concluyó demostrando que la implementación de un modelo de seguridad de la información basada en la norma ISO/IEC 27001:2013 influye positivamente en la mitigación de los riesgos de los activos de información en la Central de Operaciones Policiales de la Región Policial Junín, ya que el nivel de concientización y percepción del personal policial sobre mitigación de riesgos preimplementación fue de 24% y postimplementación fue de 99%, lo que permite señalar que este tipo de estrategias de protección resultan beneficiosas para respaldar los datos frente a posibles ataques externos, y de igual manera mantener un soporte en caso se presenten problemas en la red interna.

En la investigación de Zúñiga (2017) se hizo una revisión de las dificultades presentes en la búsqueda de instaurar estrategias de mejoramiento a la Ciberdefensa de

la información del Ejército del Perú, teniendo como caso principal: COPERE-2013-2014, donde se buscó identificar las posibles causas la desprotección y a partir de ello solucionar las deficiencias. La investigación empleí una metdología de tipo aplicada y nivel explicativo, empleando como técnica de recolección de datos el análisis documental. Asimismo, se desarrolló como instrumento un cuestionario de 48 personas, entre las cuales se encontraban autoridades, personal militar y civil encargadas del área. Entre los resultados obtenidos lo logró notar que el 68,75% desconoce la capacidad de prevención, el 66,67% la capacidad de defensa, el 77,08% la capacidad de defensa y el 75% la capacidad de respuesta. Asimismo, tras analizar los datos y procesarlos en el software estadístico SPSS se pudo notar que con un valor de 0,809 en la correlación de Spearman, se validó la hipótesis que señala que "Se observa desconocimiento o aplicación inadecuada de los procedimientos de seguridad informática; por no contar con un adecuado nivel de conocimiento de los Conceptos y Principios básicos relacionados con Ciberdefensa", lo que permite concluir señalando el grave estado de la ciberseguridad en esta entidad nacional y la necesidad de retomar los planes capacitación en lo temas relacionados, así como efectuar la Norma Técnica Peruana NTP/ISO/IEC 17799 para mejorar la protección de la información del Ejército del Perú.

2.2. INTERNACIONALES

En la investigación de Morales Cuásquer (2018) se buscó hacer una revisión de los principios de confidencialidad y transparencia ofrecida en el Centro de Apoyo a La Mediación y Negociación del Distrito Metropolitando de Quito, para lo que se empleó una metodología explicativa descriptiva, siendo el método de recolección de información una encuesta dirigida al personal administrativo, técnico y de apoyo de la institucions siendo en total 40 individuos. Asimismo, para complementar la información se contó con la revisión de estadisticas relacionadas a sus funciones. Entre los resultados obtenidos se

logró notar que un 95% del personal encuestado considera importante y beneficioso crear acuerdos de confidencialidad que ayuden a evitar la vulneración a los principios de confidencialidad en el centro estudiado. Por otra parte, un 85% señaló que en casos donde se necesite la intervención de integrantes del personal a un procesos judicial, estos deben ser inhabilitados para no presentar faltas a los acuerdos de confidencialidad internos, esto con la finalidad de protegerlos en caso sean llamados juicio como testigos, pues estos deben mantener la debida reserva de infomración bajo su cargo.

Asimismo, en la investigación de Sánchez González (2019) se buscó desarrollar un plan de mejoramiento para garantizar la confidencialidad de la infomración dentro de la empresa ECORED S.A.S. Es por ello que se contó con una investigación de carácter exploratoria, basandode en 6 etapas: Observación, recolección, análisis, diagnóstico, desarrollo y conclusión, complementando la información obtenida con la aplicación de entrevistas en una muestra compuesta por el gerente, ingeniero de sistemas, ambiental, la secretaria, adminisrtrador de empresas y contador. Tras la revisión de información, se logró notar que el conocimiento de estrategias sobre la protección de datos confidenciales se distribuye en un 4% como excelente, 23% como bueno, 19% no tiene conocimiento, 18% deficiente y el 37% es regular, de esta manera se puede concluir resaltando la necesidad de realizar un monitoreo constante de labores y responsabilidades asignadas a cada integrando, e igualmente complementar estas acciones con audtorias técnicas que señalen las deficiencias a corregir para que se puedan corregir los errores identificados.

Costales Espinoza (2021) tuvo como objetivo principal desarrollar un plan de seguridad informática que permita la confidencialidad, integridad y disponibilidad de la infromación dentro del Juzgado de la Niñez y Adolescencia de la ciudad de Quito. El plan se desarrolló considerando la legislación actual, siendo su metdología cuasi-experimental, con la investigación de tipo: de campo, bibliográfica, descriptiva y experimental. Se contó

una muestra de 25 funcionarios, los cuales pasaron por una entrevista de donde se logró obtener como resultado que un 48% desconoce las políticas de seguridad de la infomración, un 20% no sabe de la existencia del área de seguridad informatica. Ante estos resultados es que concluye señalndo la necesidad de planificar y analizar la implementación de controles de seguridad, de done se puedan considerar lo puntos débiles y vulnerabilidades en el sistema, de esta manera garantizar la protección de datos y disponibiliad de información, lo que garantizaría la confiabilidad en la empresa.

Finalmente tenemos a Silva Vieira (2016) que señala la obligación del estado a resguardar el derecho a la protección de datos como también promover la información pública a niveles de gestión, por lo que se propone la aplicación del portal "Dato Seguro" como parte de la Dirección Nacional de Registro de Datos Públicos, donde el ciudadanos podrá ver qué datos son conocidos por las entidades, de esta manera dar acceso a la información pública. El estudio comprendió de un enfoque mixto, de nivel exploratorio descriptivo y explicativo, llegando a contar con 388 ciudadanos como muestra, entre los que se encontraron habitantes de la localidad de Ambato, funcionarios de la dirección regional y expertos en seguridad informática. A estos se les aplicó una encuesta como instrumento de investigación, de donde se logró identificar el desconocimiento del portal Dato Seguro en un 74%, y asimismo un 69% desconocía las instituciones del estado que registraban su información. Ante la información ofrecida sobre el portal, in 66% se señaló en desacuerdo respecto a la posibilidad de almacenar los datos de sus bienes y patrimonio presente en el portal público. Es así como se concluye señalando la necesidad de capacitar a los funcionario públicos como a los ciudadanos en seguridad informática, pues es importante que se conozcan las obligaciones del estado respecto al derecho a la intimidad y las acciones que violentan su protección para tomar acciones contra las instituciones que gocen de nuestros datos.

III. DESARROLLO DEL TEMA (BASES TEÓRICAS)

- **DOCTRINA**

Según el autor Catino Hueso (2018), el acuerdo de confidencialidad está conformado por normas de los sujetos que brinda la información, los cuales piden que no sea revelada a terceras personas, ya que se busca proteger la identidad de la persona que está brindando dicha información. Asimismo, en el aspecto contractual, se busca que la información de los contratos no sea ventilada para poder concluir de manera óptima el contrato. Así mismo el acuerdo de confidencialidad tiene algunos parámetros que cumplir para que se lleve a cabo:

a. Tipificar el contenido que será confidencial
b. Declarar la razón por la cual la información ya no es confidencial
c. Acciones o factores por la cual la información puede ser publica o si es requerida en un proceso judicial
d. Términos generales del acuerdo de confidencialidad, como la permanencia, leyes que protegen.

El acuerdo de confidencialidad en el aspecto de mediación es de gran importancia, ya que este permite generar confianza en ambas partes, generando que se brinde información con certeza y sincera. Asimismo, se busca que ambas partes brinden los interés y necesidades que desean, esto sin ser ventilado a terceras personas y solo es utilizado para determinar el juicio (Cotino Hueso, 2017).

El acuerdo de confidencialidad posee un factor positivo y negativo, el cual señala que el positivo permite reservar la información en secreto sobre la mediación o desarrollo de un contrato a establecer, brindando la total seguridad a ambas partes en el estudio. En el sentido negativo, se plantea en que ambas partes reconozcan que no se puede divulgar

la información, datos o cualquier tema que se llevó a cabo bajo el acuerdo de confidencialidad (Santi, 2016).

Asimismo, señaló que en las reuniones de mediación los profesionales deben poseer un correcto manejo de las éticas profesional, las cuales les permitan mantener confidencialidad en obligación sobre las reuniones jurídicas; permitiendo que el proceso sea adecuado y seguro para ambas partes.

En continuación con el autor, también indicó que el acuerdo de confidencialidad y el secreto profesional son conceptos muy similares, ya que en ello se interviene la profesión de abogados, policías, notarios, etcétera, identificando que el acuerdo de confidencialidad es un acto en donde se establece parámetros y medidas para que el infórmate y los receptores no puedan revelar la información brindada. Por otro lado, el secreto profesional es la obligación o un derecho que tienen las personas que recurren a ellos.

Por otro lado, la confidencialidad en un ámbito laboral debe ser de manera equitativa, la cual no pueda ser divulgada. Asimismo, se reconoce que el poseer información sobre otras personas en manera de confidencia, genera que este posea ventaja sobre otros; es por ello que se llama a la acción el acuerdo de confidencialidad, permitiendo que las personas estén seguras sabiendo que la información está protegida por un compromiso y leyes en la cual se asegura de evitar a divulgación de la información (Quiroz Papa de García, 2016).

Asimismo, se entiende que es la garantía que genera seguridad a la otra parte, ya que la confiablidad resguardo en la información, evitar la divulgación sin el consentimiento de la persona. Siendo así que este compromiso está protegido mediante leyes que amparan en la seguridad de la información brindada por el ciudadano (Gobierno de México, 2017).

Señalando también que el acuerdo confidencial varia en los términos de legalidades y de protección según al tipo de industria que se enfocara. Lo cual mediante el acuerdo no solo se determinará en cumplir con la formalidad legal, sino también al entorno del área enfocado y la clase de información que se brindará, siendo así ser usual que se plantee como datos confidenciales la información de documentos, tratados, estadísticas financieras, información comercial; toda clase de información que vincule conocer a la otra parte.

Para establecer un correcto acuerdo de confianza se debe plantear las siguientes normas:

a. Poseer los datos e información de identidad a las personas o institución que se le brindara la información confidencial.
b. Se tipificará el tipo de información que será brindada.
c. Se establecerá el tiempo que durará el acuerdo confidencial.
d. Se tomará medidas de seguridad al momento de brindar la información y al finalizar.
e. Se da a conocer las prohibiciones que tiene la otra persona con respecto a la información brindada.

Por otro lado, el acuerdo de confidencialidad en el sector de Inteligencia Policial se identificó que brinda mayores beneficios a los colaboradores para poder efectuar de manera rápida las investigaciones criminales o ser dirigía a inteligencia contra crímenes. Siendo así que se requiere de rapidez para poder recaudar las declaraciones de las personas, en donde se le brindará total seguridad y la información recolectada servirá para los casos a desarrollar, lo cual debe estar consentida por el informante.

Ramírez (2021) mencionó que el acuerdo de confidencialidad es un contrato en donde una o varias partes lo firman en la cual es ahí donde se comprometen a mantener

la información en secreto, por ello cuando firman las partes, estas acuerdan en respetar la confidencialidad de información entre las partes que participaron, donde establecieron a no revelar información a otras personas o entidades.

Por tal motivo, al firmar el acuerdo de confidencialidad de la información, se llega a establecer entre las partes mantener en secreto el cuerdo, mientras permanece la relación entre los sujetos, y también incluso al momento de la finalización del acuerdo. Por ello se debe firmar el acuerdo de confidencialidad, esto cuando se comparte acerca de las siguientes informaciones como:

- Información comercial, como el *Know How* (conjunto de conocimientos técnicos) que puede ser secretos como la receta o código de un software, asimismo puede ser las características que se emplearan en algún diseño para ser lanzado en el futuro, una marca o logo en proceso de registrar, información financiera o contable, etcétera.
- Información industrial, científica, técnica o tecnológica con respecto a las invenciones o modelos sin patentar, en la cual hay que resaltar que el acuerdo de confidencialidad no ofrece la misma protección que una patente.
- La confidencialidad de datos personales (Ramírez, 2021).

Por otro lado, Bleda et al. (2018) manifestaron que este acuerdo de confidencialidad suele desarrollarse con un carácter previo de formalidad a la celebración del contrato de servicios, de tal manera que en el acuerdo se debe de fijar un plazo lo tiene que ser lo suficientemente amplio y a la vez protector acerca de los intereses de ambas partes sobre la información revelada entre ellas o intercambiaría, por lo cual, durante el contrato ambas partes tienen la obligación de mantener la confidencialidad.

Por ello, se describen los objetos con respecto a las cláusulas de confidencialidad, pudiendo ser lo siguiente:

- Que se proteja la información de acuerdo con las medidas correspondientes en relación con la naturaleza de información.
- Se debe tener en cuenta que la información sea confidencial durante el plazo que pacten las partes.
- Que la información sea utilizada sola para el fin determinado que se estableció en la relación contractual.
- No sea divulgada a terceras personas, ni reproducida sin que no tenga la autorización de la otra parte.
- Que la información sea destruida esto por parte receptora o devuelta al término del plazo del contrato o cuando este lo requiera.
- Que las obligaciones de confidencialidad estén sometidas durante el plazo de vigencia.
- Que las partes cumplan con las restricciones de confidencialidad de acuerdo con el contenido del contrato (Bleda et al., 2018).

En el acuerdo de confidencialidad es muy importante poder determinar acerca de que información se puede revelar y la forma de entrega, de tal manera que esto constituye como el objeto del acuerdo entre las partes, en donde esto también recae obligaciones las cuales se tendrán que cumplir, esto como el acuerdo en donde la información no sea revelara y otras que se relacionen con respecto al objeto del acuerdo. De tal manera que se deberá incluir también la responsabilidad por violar el acuerdo y tendrá que asumir las consecuencias que genere ello, en la cual, a modo de ejemplo, puede ser la inclusión de una cláusula penal (Buelvas Fattoni).

Asimismo, se tiene que tener en cuenta que dependiendo de cada legislación aplicable donde el acuerdo no se podrá violar acerca de las normas del país donde las partes han celebrado, en caso las partes tienen como domicilio principal en diferentes

países, es ahí cuando las partes deberán de especificar en el acuerdo acerca de la legislación aplicable, para evitar de esta manera inconvenientes ante futuros conflictos y así mismo evitar acerca de que ley es aplicable. Por ello, la consecuencia que podría generar por el incumplimiento del acuerdo de confidencialidad, si es que esto trae como causa un perjuicio a la otra parte, deberá de indemnizar a la parte afectada, y si en el acuerdo consagraron sanciones, también se tendrá que responsabilizar. Por ello, es esencial la determinación de una clausula penal, en estos tipos de acuerdos (Buelvas Fattoni).

Asimismo, La ley N° 29733 en su título I artículo 4 hasta el artículo 11 abarca sobre los principios rectores, para la protección de datos personales los cuales son los siguientes:

- **Principio de legalidad**

Para el tratamiento acerca de los datos personales, se tienen que establecer conforme a la ley. Por lo tanto, se prohíbe la recopilación de los datos personales esto por medio de actos fraudulentos, desleales o ilícitos.

- **Principio de consentimiento**

Es donde se debe mediar el tratamiento de datos personales de forma lícita cuando el titular hubiere prestado su consentimiento de forma libre, expreso, informado e inequívoco.

- **Principio de finalidad**

Los datos personales deben ser reunidos con una finalidad determinada, explícita y lícita, de tal manera que el tratamiento de los datos personales no debe ser para otra finalidad que no haya sido establecida de manera indudable como en el momento de la recopilación, de tal forma excluyendo los casos como las actividades en relación del valor histórico,

estadístico o científico cuando abarque la utilización de un procedimiento de anonimización.

- **Principio de proporcionalidad**

Este abarca el tratamiento de los datos personales donde debe ser adecuado, relevante y no excesivo teniendo la finalidad para lo cual hubiesen sido recopilados.

- **Principio de calidad**

Es donde los datos personales que vayan a ser tratados donde estos deben ser veraces, exactos, y sobre todo actualizados. Por lo cual, se debe de conservar como garantía la seguridad de los datos personales recopilados.

- **Principio de seguridad**

El titular del banco de datos personales y también el encargado acerca del tratamiento donde deben adoptar las medidas técnicas, organizativas y legales esto para garantizar la seguridad de la información acerca de los datos personales, por lo que estas medidas deben de ser muy idóneo y adecuado con el tratamiento que se efectué.

- **Principio de disposición de recurso**

Es donde todo titular de datos personales, este debe contar con las vías administrativas o jurisdiccionales necesarias para que pueda reclamar y hacer valer sus derechos cuando haya sido vulnerado su derecho.

- **Principio de nivel de protección adecuado**

Para la realización del flujo transfronterizo acerca de los datos personales, este se debe de garantizar la mayor protección para los datos personales que se vayan a tratar, en la cual

debe estar por lo menos equiparable con lo establecido por esta ley o los estándares internacionales respecto a la materia (Congreso de la República, 2011).

- **LEGISLACIÓN**

Ley de protección de datos personales- Ley N° 29733

La ley de protección de datos personales tiene por finalidad de resguardar los datos e información brinda de los ciudadanos, lo cual puede ser pedido como medio de prueba o testigo ante un crimen. Señalando que la Ley es aplicable ante cualquier órgano público y privado; permitiéndole al ciudadano permanecer seguro en la sociedad (El peruano, 2017).

Artículo 17 – Confidencialidad de datos personales

El profesional encargado de estar presente en la entrega de información con el ciudadano, está comprometido por obligación a brindar confidencia ante los hechos comentados. Asimismo, este no puede divulgar a terceras personas, lo cual puede ser posible si el ciudadano brinda el consentimiento de hacerlo.

Artículo 32 – Confidencialidad y seguridad

Con relación a los medios de comunicación estos tienen la obligación de brinda seguridad, y confidencialidad a los usuarios que recurren a sus dispositivos; siendo así que estos no podrán usar o indagar en la información que estos bridan. Siendo estas medidas resguardadas por la Ley.

Artículo 35 – Confidencialidad

La persona con autoridad nacional con deber de protección de datos personales, tiene la obligación de brindar confidencialidad sobre la información que posee, esto es aplicado para la información de ciudadanos comunes o de su entorno. También se señala

que la obligación y compromiso en brindar confidencialidad es aplicado durante la etapa de trabajo y cuando esté ya cesa de trabajar en ese puesto.

Ley de Información No Divulgada

Artículo 1 – Objeto

Se plantea como finalidad el poder informar sobre las normas establecidas en la Ley de Información no Divulgada, Ley N° 7975, viéndose reflejadas en el área de registros de propiedades; en donde se requiere de confidencialidad en algunos aspectos de los documentos y otros son parte público por orden de la Ley.

Artículo 2 – Ámbito de protección

Se requiere seguridad ante los datos no divulgados sobre las industrias, empresas o tratados entre ellos, aplicando la Ley N° 7975, la cual brinda mayor seguridad y confianza en el desarrollo de un contrato. Asimismo, se señala que siendo un acuerdo privado y de confidencialidad ambas partes deben estar en el proceso de comercialización, desarrollo.

Artículo 7 – Protección de la información no divulgada en procedimiento judiciales

Las autoridades que velan por la protección de la información brindada tienen por obligación el dar a conocer y establecer los parámetros para evitar que cualquier de las ambas partes divulguen información confidencial sobre el desarrollo de la Industria y no usen de ella. También la autoridad judicial puede decidir evitar de comentar sobre algunos datos de confidencia, si esto parece información irrelevante para el caso.

- **JURISPRUDENCIA**

Mediante la corte Suprema de San José, teniendo por expediente el Caso N° 96-001309-0185-LA, en donde se desarrolló el caso de Laboratorios Griffth de

Centroamérica sociedad quien fue demandado por el actor Roberto Suñol, llevándolo a un caso judicial por la falta de compromiso e incumplir con las normas en el contrato de confidencialidad establecido previamente a los hechos, añadiendo que es un Laboratorio profesional el cual da a entender que hizo falta de ética y compromiso profesional. Siendo así que el actor requiere que el Laboratorio Griffth brinde una indemnización por los daños realizados hacia su persona y su familia. Añadiendo que en el proceso se hizo nula la confidencialidad establecida entre ambos, con el objetivo de poder declarar ampliamente con sus abogados y así mismo con el juez.

Siendo así que, mediante las Leyes y normas establecidas en el acuerdo, es el cual permite que brinde seguridad sobre las declaraciones y protejan los derechos de la víctima, por el cual el Juzgado determino la aprobación de la petición del actor; dando a conocer que Laboratorio Griffth no cumplió con las Leyes de confidencialidad. Asimismo, que carece de compromiso y confidencialidad profesional.

- **TRATADOS**

Observándose en el CIJUL de Colegio de Abogado y Abogadas de Costa Rica, en donde plantearon como tratado de confidencialidad ante la información de los casos que estos poseen por la profesional que ejercen, siendo así que se aplicara sanciones ante el profesional que revelan información confidencial. Procurando brindar mayor seguridad y confianza a los usuarios mediante la aplicación de la Leyes y normas en beneficio de los derechos de las personas.

Se señala que en 1995 en Bruselas se estableció el primer convenio de la Policía Europea el cual fue denominado “Convenio Europol”. Comenzando con las labores en 1999, mediante este convenio se pudo abarcar mayor campo de Intervenciones policiales, brindando seguridad en la ciudad. Asimismo, se estableció en los procesos confidencialidad en los casos de los agraviados un mejor planteamiento de seguro sobre

la información a brindar, permitiendo que este pueda descargar toda la información necesaria para la lucha del caso; además en donde los efectivos policiales mediante este Convenio fueron capacitados y pasaron por pruebas para medir su nivel de compromiso y confidencialidad profesional, brindándole mayor seguridad a los ciudadanos (Goizueta Vértiz, 2017).

IV. CONCLUSIONES

En la primera conclusión, la confidencialidad de datos personales se encuentra regulado en el la Ley N° 29733 dentro del artículo 17 que abarca acerca de la obligación que tiene el titular a no divulgar información a terceras personas, esto sin el consentimiento alguno, por ello, es un derecho que se tiene que guardar como secreto profesional.

Como segunda conclusión, la mencionada Ley de protección de datos personales abarca 12 principios rectores para la protección de datos, las cuales son los siguientes principios: legalidad, consentimiento, finalidad, proporcionalidad, calidad, seguridad, disposición de recurso, nivel de protección adecuado y valor de los principios.

En su tercerea conclusión, en los países como Colombia y Ecuador dentro de su normatividad legal, abarca el principio de confidencialidad, donde todas las personas que realicen o intervengan en los datos personas, sin que tenga naturaleza de carácter público, están obligadas a reservar dicha información.

Por último, en su cuarta conclusión, mediante el requerimiento de la Policía Nacional sobre las declaraciones de los agraviados o personas cercanas a ellas a un investigado, se establece mediante la Ley la total seguridad durante el llamado y durante un tiempo pactado por ambos. Siendo esta información utilizada para realizar investigaciones criminales o directamente a equipo de inteligencia; asimismo, se requiere de la autorización del colaborador para utilizar esta información. Además, en donde los efectivos policiales poseen el compromiso de no ventilar información alguna de las acciones que se desarrollan.

V. APORTE DE LA INVESTIGACIÓN

Para el presente estudió en investigación, en su **justificación práctica**, la presente investigación tiene por objetivo el poder analizar el acuerdo de confidencialidad en la DIRTIC de la Policía Nacional del Perú, 2021. De igual manera, brindando información para el conocimiento de los ciudadanos.

Por otro lado, en su **justificación teórica**, en la investigación se desarrolló el tema de Análisis del acuerdo de confidencialidad, siendo así que se necesitó de antecedentes internacionales y nacionales permitiéndonos plantear de manera clara el tema de estudio, además se requirió de artículos científicos, indexados, Leyes y normas, dando mayor aporte al desarrollo del estudio. Teniendo como objetivo teórico que este estudio pueda ser utilizado como antecedente o para ampliar los conocimientos de los estudiantes.

VI. RECOMENDACIONES

Como primera recomendación, es necesario que toda información que se presente ante la Policía Nacional del Perú tenga un acuerdo de confidencialidad entre las partes, con el fin de asegurar la información que esta regula por la Ley N° 29733, con ello se obligan entre las partes a no divulgar información, como también no revelar datos sin consentimiento alguno de ambas partes. Por ello, también se protege la seguridad de los derechos personales de ambas partes.

En su segunda recomendación, es necesario implementar en los acuerdos de confidencialidad con la PNP, los principios rectores que rige la Ley N° 29733 para tener un respaldo acerca de la protección de datos. Esta estrategia parte desde los principios de protección y la adecuada manipulación de datos, por lo que tanto entidades públicas o privadas se encuentran comprometidas a tomar las acciones de prevención necesarias para evitar vulnerabilidades que afecten la información personal y sancionar a los integrantes que busquen atentar contra estos derechos.

En su tercera recomendación, es importante poder implementar en los principios rectores, el principio de confidencialidad, así como lo contiene los países de Colombia y Ecuador dentro de sus normas legales, para la protección de los datos personales de la persona. Esto a través de estrategias de reforzamiento que recalquen las consecuencias de actos que vulneren estos principios, junto con estrategias institucionales que recalquen su importancia, incitando a manipularlos con cautela en las áreas competentes.

Por último, en su cuarta recomendación, es necesario poder implementar en los acuerdos de confidencialidad y cláusulas penales, para cualquiera de las partes que incumpla acerca del acuerdo, para tener una mejor seguridad de los datos de información, evitando así que se divulgue información confidencial y se logre imponer sanciones ejemplares al vulnerar estos derechos.

VII. REFERENCIAS BIBLIOGRÁFICAS

Bleda Navarro, G. M., Bulnes Fernández-Mazaramboz, D., Márquez Salas, S., Mata Gonzáles, M. Á., Minero Alejandre, G., Muñoz Rodríguez, J., . . . Suárez Jaqueti, H. (2018). *Guía para la redacción y negociaciación de contratos de software*. DENAE. https://www.wipo.int/export/sites/www/amc/en/docs/denaeguia2018.pdf

Buelvas Fattoni, M. A. (2017). Acuerdo de confidencialidad. *Universidad CES*. https://repository.ces.edu.co/handle/10946/3594

Catino Hueso, L. (2018). Confidencialidad y protección de datos en la mediación en la Unión Europea. *IUS. Revista del Instituto de Ciencias*. https://www.redalyc.org/pdf/2932/293258387017.pdf

Chávez Rodríguez, E. G. (2018). *El delito contra datos y sistemas informáticos en el derecho fundamental a la intimidad personal en la Corte Superior de Justicia de Lima Norte, 2017* [Tesis de doctorado, Universidad Nacional Federico Villarreal]. http://repositorio.unfv.edu.pe/handle/UNFV/2704

Chilán-Santana, E. I. y Pionce-Pico, W. F. (2017). Apuntes teóricos introductorios sobre la de la información. *Ciencias Informáticas*, *3*(4), 284–295. https://dialnet.unirioja.es/servlet/articulo?codigo=6174477

CIJUL en linea. Centro de Información Jurídica en Línea. (2008). El Contrato de Confidencialidad en el derecho Costarricense. *CIJULenlinea*. https://cijulenlinea.ucr.ac.cr/2008/el-contrato-de-confidencialidad-en-el-derecho-costarricense/

Cotino Hueso, L. (2017). Confidencialidad y protección de datos en la mediación en la Unión Europea. *Revista IUS*. https://www.redalyc.org/journal/2932/293258387017/293258387017.pdf

El peruano. (2017). Ley de Protección de datos personales Ley N° 29733. *El peruano*. https://diariooficial.elperuano.pe/pdf/0036/ley-proteccion-datos-personales.pdf

Galarza Guerrero, S. E. (2018). *La confidencialidad versus el derecho de acceso a la información en la mediación del sector público* [Tesis de licenciatura, Universidad San Francisco de Quito USFQ]. https://repositorio.usfq.edu.ec/bitstream/23000/7789/1/140789.pdf

Gobierno de México. (2017). Confidencialidad d ela información. *INCMNSZ*. https://www.incmnsz.mx/opencms/contenido/investigacion/comiteEtica/confidencialidadInformacion.html

Goizueta Vértiz, J. (2017). La cooperación policial en el seno de Europol: El principio de disponibilidad y la confidencialidad de la información. *Revista Española de Derecho Constitucional*. https://dialnet.unirioja.es/servlet/articulo?codigo=6112334

González Candia, J. C. (2018). *Tratamiento de los acuerdos de confidencialidad en los contratos de trabajo: ¿una solución al secreto empresarial en la etapa post contractual de la relación laboral?* [Tesis de maestría, Universidad de los Andes de Colombia]. https://repositorio.uniandes.edu.co/handle/1992/34550

Goyzueta Vértiz, J. (2017). La cooperación policial en el seno de europol: el principio de disponibilidad y la confidencialidad de la información. *Revista Española de Derecho Constitucional*, *110*, 75–104. https://www.jstor.org/stable/26375297

Jaramillo Baanate, M., & Campos Ugaz, D. (2019). *Contratos laborales en el Perú: dinámica y determinantes.* GRADE. https://www.grade.org.pe/wp-content/uploads/GRADE_di98.pdf

Ley Estatutaria 1581 de 2012. (2012, 17 de octubre). Congreso de Colombia. Diario Oficial.

Ley N° 29733. (2011, 3 de julio). Congreso de la República. El Peruano. https://www.gob.pe/institucion/congreso-de-la-republica/normas-legales/243470-29733

Ley Orgánica de Protección de Datos Personales. (2021, 26 de mayo). República de Ecuador. Registro Oficial Suplemento No. 459. https://www.consejodecomunicacion.gob.ec/wp-content/uploads/downloads/2021/07/lotaip/Ley%20Org%C3%A1nica%20de%20Protecci%C3%B3n%20de%20Datos%20Personales.pdf

Martín-Retortillo, M. R. (2020). Secreto, transparencia, confidencialidad y protección de datos en la contratación pública. Estudio de las resoluciones de los tribunales administrativos de contratación y del consejo de transparencia y buen gobierno y órganos equivalentes. *Anuario da Facultade de Dereito da Universidade da Coruña, 24*, 150-191. https://ruc.udc.es/dspace/bitstream/handle/2183/27823/7.-%20Rodr%c3%adguez%20Mart%c3%adn-Retortillo%20CON%20DOI.pdf?sequence=1&isAllowed=y

Niño Morante, N. R. (2019). *Modelo de un sistema de gestión de seguridad de información – SGSI, para fortalecer la confidencialidad, integridad, disponibilidad y monitorear los activos de información para el Instituto Nacional de Estadística e Informática - INEI filial Lambayeque* [Tesis de maestría,

Universidad Nacional Pedro Ruiz Gallo]. https://repositorio.unprg.edu.pe/handle/20.500.12893/5935

Quiroz Papa de García, R. (2016). El Hábeas Data, protección al derecho a la información y ala autodeterminación informativa. *Revista de Derecho de la Pontificia Universidad Católica de Valparaíso*. http://www.scielo.org.pe/pdf/letras/v87n126/a02v87n126.pdf

Ramírez, H. (2021). El acuerdo de confidencialidad (NDA). Todo lo que necesitas saber. Grupo Atico34. https://protecciondatos-lopd.com/empresas/acuerdo-de-confidencialidad-nda/

Registro Nacional de Costa Rica. (2009). Reglamento a la Ley de Informacón No Divulgada. *Registro Nacional de Costa Rica*. http://www.registronacional.go.cr/propiedad_industrial/documentos/pi_normativa/decretos/informacion%20no%20divulgada.pdf

Santi, M. (2016). Controversias éticas en torno a la privacidad, la confidencialidad y el anonimato en investigacion social. *Revista de Bioética y Derecho*. https://www.redalyc.org/pdf/783/78346079002.pdf

Zacarias Villafranca. J. C. (2017). *Modelo de seguridad de la información basado en la ISO/IEC 27001:2013 para mitigar los riesgos de los activos de información en la Central de Operaciones Policiales de la Región Policial Junín* [Tesis de grado, Universidad Continental]. http://repositorio.continental.edu.pe/handle/continental/4105

Anexo: Carta de Autorización de Nombre

PERÚ | Ministerio del Interior | Policía Nacional del Perú | Secretaría Ejecutiva PNP | Dirección de Tecnología de la Información y Comunicaciones PNP

"Año del Fortalecimiento de la Soberanía Nacional"

Lima, 08 de febrero de 2022

Señores:
UNIVERSIDAD PERUANA DE LAS AMÉRICAS

Asunto: autorización de uso de nombre de la empresa y aplicación del cuestionario.

Estimados, señores me dirijo a ustedes en mi calidad de Director de Tecnología de la Información y Comunicaciones de la Policía Nacional del Perú a fin de autorizar al sr(srta) Marilyn Del Carmen VALENZUELA NEYRA quien es alumna de la carrera de Derecho de su prestigiosa universidad, el uso del nombre de nuestra institución y, asimismo, la aplicación del cuestionario de la investigación que lleva por título: ANÁLISIS DEL ACUERDO DE CONFIDENCIALIDAD EN LA DIRECCIÓN DE TECNOLOGÍA DE LA INFORMACIÓN Y COMUNICACIONES DE LA POLICÍA NACIONAL DEL PERÚ(DIRTIC PNP), 2021.

Cabe señalar, que toda esta información debe ser uso únicamente con fines académicos.

Sin otro particular, me despido de ustedes. Agradeciendo por su amable atención.

Atentamente,

FIRMA
Nombre y Apellido Raúl Arnaldo SILVA OLIVERA
DNI 09992949