# UNIVERSIDAD PERUANA DE LAS AMÉRICAS

**ESCUELA DE DERECHO**

**TESIS**

# “La incidencia de los delitos informáticos en la implementación progresiva del plan de gobierno digital de OSITRAN 2019-2022”.

PARA OPTAR EL TÍTULO PROFESIONAL DE ABOGADO


AUTOR:

ANIBAL RAUL ALIAGA SWIDIN

ASESOR:

DR. AARON OYARCE YUZZELLI


LÍNEA DE INVESTIGACIÓN: DERECHO PENAL Y PROCESAL PENAL

LIMA-PERÚ

DICIEMBRE, 2019

## Dedicatoria

A mi padre Anibal, por la magistral conducción de su linaje, señalando el derrotero a seguir y preservando la unidad de la familia. A mi mamá Chela, por ser un dechado de ternura y abnegación para con sus hijos y nietos. A mi madre biológica Svetlana que me da fuerzas desde el infinito. A Carla, por ser la entrañable compañera que siempre está ahí.

A mis queridos hijos Anibal Gianmarco, Catalina Svetlana e Ignacio Julián, por ser soplos de energía e ilusión para forjar un futuro mejor.

## Agradecimientos

Mi reconocimiento y agradecimiento especial a mis señores padres, quienes, a lo largo de mi travesía estudiantil, siempre estuvieron presentes con su apoyo y confianza incondicional, estímulos que me permitieron avanzar y concluir exitosamente mis estudios; dando así el primer paso para seguir tras las huellas dejadas por mi padre, desafío que asumo con el sagrado compromiso que corresponde a la estirpe de los Aliaga.

Asimismo, extiendo mi agradecimiento profundo a mis tíos, hermano, esposa e hijos por sus alientos y ánimos que valoro en su real magnitud.

Finalmente, abrazos de agradecimientos a mis amigos, quienes de una u otra forma me expresaron su adhesión y respaldo, que fueron determinantes para llegar a la meta.

**Resumen:**

La presente investigación estudia el tema de los delitos informáticos y el gobierno digital con el propósito de resolver el problema principal de la investigación, siendo este determinar qué factores de los delitos informáticos inciden en la implementación progresiva del plan de gobierno digital de OSITRAN 2019-2022. En efecto, se realizará un trabajo desde la perspectiva teórico, práctico, jurídico y social, de forma tal que pueda hallarse una explicación al como las acciones antijurídicas contra los datos y sistemas informáticos, contra el patrimonio y la fe pública, en su calidad de factores, afectan al proyecto de gobierno digital de OSITRAN, generando así un clima de ausencia de ciber-seguridad. Siendo así, la presente investigación posee como objetivo determinar qué factores de los delitos informáticos inciden en la implementación progresiva del plan de gobierno digital de OSITRAN 2019-2022 y como hipótesis principal, el que los delitos informáticos afectan negativamente al plan de gobierno digital de OSITRAN 2019-2022, la cual será contrastada a lo largo de la investigación. Para lograr ello, se analizará el marco nacional, comparado, supranacional, conceptos vinculados a los delitos informáticos y gobierno digital, las estipulaciones del proyecto de OSITRAN en materia de gobierno digital y la consulta a conocedores de la materia para verificar si, efectivamente, se ha producido dicha incidencia al marco digital que OSITRAN busca implementar, durante el rango de tiempo 2019-2022. Asimismo, es de señalar que la investigación es de carácter mixto, correlacional, descriptivo, exploratorio, experimental y emplea un método de carácter inductivo.

**Palabras clave:**

Delitos informáticos-gobierno digital-OSITRAN-acción antijurídica-ciber-seguridad.

**Abstract:**

This investigation studies the issue of cybercrime and digital government in order to solve the main problem of the investigation, this being to determine what factors of computer crime impact on the progressive implementation of OSITRAN's digital governance plan 2019-2022. Indeed, work will be carried out from a theoretical, practical, legal and social perspective, so that an explanation can be found such as anti-legal actions against data and computer systems, against heritage and against the public faith, as factors, affect OSITRAN's digital governance project, thus creating a climate of no cyber-security. Thus, the general objective of this investigation is to determine which factors of computer crime impact on the progressive implementation of OSITRAN's digital governance plan 2019-2022 and as a main hypothesis it has been raised that computer crimes adversely affect OSITRAN's digital governance plan 2019-2022, , which will be tested throughout the investigation. To achieve this, the national, comparative, supranational, computer crime and digital governance framework will be analysed, OSITRAN's digital governance project and consultation with those inthe field to verify whether there has indeed been such an impact on the digital framework that OSITRAN seeks to implement during the time range 2019-2022. It should also be noted that the research is of a mixed, correlational, descriptive, exploratory, experimental nature and employs an inductive method.

**Keywords:**

Cibercryme-digital government-OSITRAN- unlawful actions-ciber security.

# Tabla de contenidos

# Lista de Tablas

# Introducción

En la actualidad, es corriente observar abundantes cantidades de investigaciones y/o estudios científicos cuya temática versa sobre los delitos informáticos. De igual manera, también es factible observar asignaciones investigativas que han dispuesto como propósito otorgar un marco de lectura sobre la concepción de gobierno digital, tanto en su versión de proyecto y sus distintas derivaciones.

Siendo así, la presente investigación busca unificar, articular, vincular las temáticas de los delitos informáticos y los proyectos de gobierno digital a fin de comprobar si, efectivamente, dichas acciones informáticas contrarias al ordenamiento jurídico disponen de un amplio margen de afectación para con los proyectos de gobierno digital que vienen implementando las instituciones públicas peruanas, en un determinado rango de tiempo (2019-2022).

A pesar de lo anterior, se debe referir que el grado de estudio se concentrará en el proyecto de gobierno digital de OSITRAN 2019-2022, en función de que sobre dicha institución ha recaído una gran controversia, una serie de cuestionamientos, debido a que, presuntamente, se habría suprimido información de connotación pública (de importante relevancia), lo cual contravendría, de comprobarse el supuesto investigado, las directrices que OSITRAN busca insertar con su proyecto de gobierno digital. Por tanto, la visión de fondo de nuestra investigación se orientará a determinar qué elementos de los delitos informáticos atentan contra las tratativas de OSITRAN por insertar, al sistema interno, su proyecto de gobierno digital 2019-2022.

Por consiguiente, el desarrollo del actual producto científico se ha estructurado en base a los siguientes capítulos:

En el capítulo I, se abordará todo lo concerniente a nuestro problema de investigación, comenzando por delinear el campo general de estudio para luego centrarnos en la disyuntiva específica (referente a si los delitos informáticos inciden en el proyecto de gobierno digital de OSITRAN 2019-2022); además, se expondrá, derivado del problema principal, problemas específicos, objetivo general y objetivos específicos, así como también se compartirán el por qué el desarrollo de la investigación es viable y útil, pero también se referirán cuáles son los obstáculos y limitaciones para su concreción.

En el capítulo II, se explicarán todos los detalles que componen a nuestro marco teórico, como la descripción de las tesis preexistentes que poseen algunos aspectos interesantes y fortalecedores para nuestras finalidades investigativas; asimismo, se señalaran un conglomerado de conceptos y nociones esenciales para comprender la investigación, derivados de las variables de delitos informáticos y gobierno digital, como el tema de la ciber-seguridad, el bien jurídico protegido, ecosistema digital de gobierno digital, un estudio nacional, comparado y supranacional de las variables del estudio, entre otros detalles; además, para aclarar alguna ambigüedad, se tipificará un agrupado de términos básicos, esenciales y reiterados en el proyecto.

En el capítulo III, se comentará todo lo concerniente al aspecto metodológico, tales como la operacionalización de las variables (indicadores y dimensiones); aunado a ello, se plantearán las hipótesis de la investigación; seguido de ello, se comentará cuál es la población y muestra efectiva del trabajo; asimismo, se explicará cuál es el método de la investigación y los instrumentos de recopilación de datos utilizados en la investigación.

En el capítulo IV, se abordará lo relativo al análisis y la interpretación de los resultados como a la respectiva discusión de los mismos, de forma tal que pueda validarse o bien desmentirse lo planteado en las hipótesis de trabajo u otros aspectos conexos a las mismas.

Por último, en la parte final del trabajo se estipularán las conclusiones y recomendaciones, las cuales recabarán la posición final que pueda determinarse en base al transcurso total de nuestro producto investigativo. No está de más dejar en claro que también se añadirá, en la parte de apéndices, lo referido al instrumento empleado para recopilar los datos como la pertinente matriz de consistencia.

# CAPÍTULO I: PLANTEAMIENTO DEL PROBLEMA

## Descripción de la Realidad Problemática:

En el hoy en día, es factible, viable el poder visualizar distintos avances en la forma de concretar las diversas acciones jurídicas y no jurídicas que se desarrollan en el día a día en las indistintas sociedades (no única y exclusivamente la peruana), ya sea en materias de los procesos de contrataciones y adquisiciones a nivel gubernamental, convenios internacionales, emisión de normas legislativas, resoluciones jurisdiccionales, las tratativas entre particulares para satisfacer específicos requerimientos de los mismos, así como el proceso de consolidación de las relaciones entre la autoridad gubernamental con los agentes con poder no estatal y/o grupos de la sociedad civil.

Pues bien, respecto al último contexto mencionado, es de señalar que uno de dichos avances lo constituye la denominada implementación del mecanismo "Gobierno digital, E-gobierno o Gobierno electrónico". Sin perjuicio de la denominación en concreto que pueda adoptarse a efectos del propósito de elaborar este trabajo, lo cierto es que el mismo ha surgido como una novedad para el proceso de construir y consolidar los vínculos entre el actor gubernamental para con las agrupaciones que cuentan con poder no estatal (como las empresas) y/o las organizaciones cotidianas de la comunidad civil. Es decir, ya sea para la tramitación de procesos, procedimientos, quejas, denuncias, reclamos, convenios u otra herramienta que requiera interacción entre el componente estatal con las empresas o sujetos civiles, sea hace posible observar una intencionalidad de sumergir dichas actuaciones a las particularidades concretas del nominado gobierno electrónico.

De esta manera, antes de continuar, es necesario disponer de una somera noción, acepción de tal gobierno electrónico, pudiendo ser concebido, desde la perspectiva de la OCDE, como el

manejo de las tecnologías de la información y comunicación (TICS), particularmente el Internet, como instrumento para lograr la optimización del gobierno; asimismo, desde la visión del Banco Mundial, puede comprendérselo como la utilización las citadas TICS, por parte de los actores gubernamentales, con la finalidad de impulsar el cambio en la comunicación entre los ciudadanos, negocios y otras extensiones del gobierno. (Naser, s.f)

En base a lo expuesto anteriormente, es razonable considerar que dichos cambios, avances, técnicas son adecuados, pertinentes, idóneos, de conformidad a la mentalidad de orientarnos a un proceso de globalizar digitalmente, a la comunidad mundial, aunque claro está que el progreso de dicha meta será proporcional a las particularidades y recursos del país concreto. En el caso peruano, para el cumplimiento de las finalidades estipuladas, tenemos a disposición el Decreto Legislativo N° 1412, directriz normativa que regula los parámetros relativos al gobierno digital en nuestro marco jurídico.

Sin embargo, si recordamos el conocido refrán “no todo es de color rosa” puede llegar a concluirse de que si bien es un ideal que los pormenores del gobierno digital prosigan su curso de estandarizarse en la sociedad, lo cierto es que dicha forma de pensar no carece de algún tipo de desarreglo (como manejos ineficientes de los instrumentos que derivan de la unidad llamada gobierno digital) o de conductas transgresoras a la conformidad de la aplicabilidad del gobierno electrónico con nuestro sistema jurídico (como el caso de los delitos informáticos).

Deteniéndonos en este último aspecto, diremos que un delito informático, en términos puntuales, es una conducta propiciadora de las llamadas vulneraciones a la ciber-seguridad. Para su materialización, también se emplean a las anteriormente mencionadas TICS, solo que, en este caso, por lógica, mientras que en el gobierno digital se las empleaba para estabilizar las relaciones y coordinaciones entre Estado y el resto de concurrentes en la sociedad, los delitos informáticos las usan para generar un perjuicio a la referida estabilidad o equilibrio digital. Al respecto de ello, la

organización gubernamental del Perú, a partir de su preocupación por este ámbito, dictaminó la entrada en vigencia de la Ley N°30096 (modificada por Ley N°30171) a efectos de regular algunos detalles sobre dicha temática.

En términos reducidos, la idea de la autoridad estatal peruana fue que la concreción de los ideales del gobierno digital, en las diferentes entidades de la administración pública sea factible, sin dejar descuidado, conforme puede desprenderse de la intención del legislador, el tema de los delitos informáticos. Prueba de ello es que entidades como el Ministerio de Economía y Finanzas, Ministerio de salud, SUNARP, OSITRAN, OEFA u otros, vienen implementando, de manera progresiva, ciertos proyectos de gobierno digital (2019-2022).

La interrogante que se plantea, en base a todas las ideas que constituyen esta sección, es si dicha inserción de tal plan de gobierno digital puede calificarse como eficiente. Vale decir, si tales programas no son ajenos a sufrir un margen de desperfecto (terminología inadecuada de alguna regla) como de un accionar que contravenga los planes de gobierno digital (delito informático) en el marco de su adopción en el sistema jurídico peruano.

A raíz de lo anterior, es que llegamos a edificar la interrogante que estructura nuestra investigación respecto a la hipotética incidencia de los delitos informáticos en el marco de la implementación progresiva de un proyecto de gobierno digital 2019-2022, en este caso, del OSITRAN. Por consiguiente, a efectos de empezar a solventar la interrogante en cuestión, compartiremos las particularidades de un reciente suceso que ha generado cierta controversia alrededor de dicha institución, en el cual se ha dado a conocer una presunta supresión de información de relevancia pública (involucrada con un delito materia de investigación por las autoridades peruanas) la cual comprometería a ciertos ex-funcionarios de dicha entidad. Esto, como es evidente, requiere analizarse a efectos de determinar si dicho acontecimiento encaja en el supuesto de hecho de algún tipo penal de la legislación de delitos informáticos. Sin perjuicio de lo

anterior, si se ha podido observar que una conducta que transgrede un todo informático y que es indispensable para fines de conocimiento público, es claro que los componentes de este suceso pueden llegar a generar cierta suspicacia tanto en los operadores jurídicos como en la población, respecto a la probable dación de un posterior ataque al sistema informático de dicha entidad, en el marco del desarrollo de su respectivo proyecto de gobierno digital.

## Formulación del Problema

### Problema General.

- ¿Qué factores de los delitos informáticos inciden en la implementación progresiva del plan de gobierno digital de OSITRAN 2019-2022?

### Problemas Específicos.

- ¿En qué medida los delitos contra los datos y sistemas informáticos influyen en la implementación progresiva del plan de gobierno digital de OSITRAN 2019-2022?
- ¿De qué manera los delitos informáticos contra el patrimonio afectan en la implementación progresiva del plan de gobierno digital de OSITRAN 2019-2022?
- ¿De qué forma los delitos informáticos contra la fe pública repercuten en la implementación progresiva del plan de gobierno digital de OSITRAN 2019-2022?

## Objetivos de la Investigación

### Objetivo General.

- Determinar qué factores de los delitos informáticos inciden en la implementación progresiva del plan de gobierno digital de OSITRAN 2019-2022.

**Objetivos Específicos.**

- Determinar en qué medida los delitos contra los datos y sistemas informáticos influyen en la implementación progresiva del plan de gobierno digital de OSITRAN 2019-2022.
- Identificar de qué manera los delitos informáticos contra el patrimonio afectan en la implementación progresiva del plan de gobierno digital de OSITRAN 2019-2022.
- Verificar de qué forma los delitos informáticos contra la fe pública repercuten en la implementación progresiva del plan de gobierno digital de OSITRAN 2019-2022.

## Justificación e Importancia de la Investigación

La presente investigación se encuentra justificada en razón de que es necesario iniciar la constitución de estudios en materia de los planes de gobierno digital, por parte de las diferentes entidades de la administración pública. Como bien se dijo, OSITRAN no es la única institución que viene apoyando la inserción de tales planes de gobierno electrónico por lo que es importante que, desde ya, se inicien las indagaciones que tengan como propósito verificar si el acomodo de los citados planes es concordante con los postulados del ordenamiento jurídico, en el sentido de respetar la legislación unificada como las expectativas ciudadanas, ya que es sabido que el manejo, proceso directivo de la sociedad se asocia con un esquema de gobernanza y no de gobernabilidad (las decisiones que sean efectivizadas deben articularse, coordinarse y ser de responsabilidad tanto del actor estatal como de la sociedad civil, debidamente representada).

Por otro lado, en cuanto a la importancia de la investigación, puede ser vista desde un factor teórico, práctico y social.

Respecto al componente teórico, puede señalarse que la importancia se visualiza en razón de utilizar ciertas particularidades conceptuales del derecho informático (gobierno digital y delitos

informáticos), para estudiar una situación novedosa que se desprende, precisamente, de los pormenores de ambas figuras teóricas.

En cuanto al elemento práctico, la pertinencia se materializa en razón de no circunscribirse nuestra visión a un enfoque eminentemente teórico, sino que, además, se trasladarán las acepciones teóricas al discurrir respecto a si los delitos informáticos, efectivamente, pueden incidir o no en la concreción de los ideales de un plan de gobierno digital de una institución de la administración pública.

Sobre el elemento social, puede decirse que esta investigación servirá como un incentivo adicional a los propósitos de combatir los indeseados efectos de los delitos informáticos, como la ciber-delincuencia, atentado a la conservación de datos de relevancia nacional, afectación de base datos de las entidades u otros derivados similares.

De otro lado, puede decirse que esta investigación es viable, ya que se cuentan con los siguientes materiales a disposición:

- Proyecto de implementación del plan de gobierno digital de OSITRAN 2019-2022
- Bibliografía enfocada en la materia de gobierno digital
- Bibliografía especializada en la temática de delitos informáticos
- Material orientado al estudio de la rama general (derecho informático)
- Proyectos de investigación (tesis) que estudian diversos aspectos del gobierno digital y delitos informáticos.
- Disposición del caso que nos permite determinar los primeros cimientos en cuanto a que los delitos informáticos sí se encuentran influyendo la ejecución proseguida del plan de gobierno digital de OSITRAN 2019-2022.

- El conocimiento y el interés sobre la temática de la presente investigación, por parte del tesista.

**Limitaciones de la Investigación**

A pesar de haber expuesto los motivos que denotan la justificación de la presente asignación investigativa, así como los hechos que constituyen la esencia de su posibilidad de ser concretada, no debe desatenderse que todo ánimo de investigación siempre estará rodeado de obstáculos para ser concretado. Por consiguiente, las limitaciones a la investigación pueden ser resumidas, como las siguientes:

- No existen estudios previos, por parte de los duchos del derecho, que se hayan orientado a examinar o emitir posiciones de debate respecto a estos planes progresivos 2019-2022 (MINSA, MINCETUR, OEFA, OSITRAN, entre otros) que buscan implementar el gobierno digital en diferentes instituciones de la administración pública.

# Capítulo II: Marco Teórico

## Antecedentes de la Investigación

### Internacionales

Cortez & Chang (2012) en su tesis titulada "Diseño de un nuevo esquema para el procedimiento de indagación de los delitos informáticos", tiene como propósito establecerse como una herramienta que coadyuve a insertar una nueva estructura que coadyuve las indagaciones sobre los delitos informáticos, en concordancia con la normativa ecuatoriana existente y pertinente sobre la materia. Para lograr ello, se emplearon un conjunto de tipos de investigación, a saber, exploratoria, descriptiva, explicativa, de campo y horizontal; asimismo, el método investigativo fue el inductivo-deductivo, analítico-sintético, comparativo y estadístico. Además, se empleó una población de 15197 personas, entre fiscales, abogados, policías u otros.

González (2013) en su tesis nominada "Delincuencia Informática: daños informáticos del artículo 264 del código penal y propuesta de reforma" dispuso como objetivo la exposición de un marco que permita visualizar la delincuencia informática en la era actual de España, enfocando en el análisis del artículo 264 de su respectivo Código Penal (delitos informáticos), a fin de comentar su respectiva realidad y proponer una manera de mejora. Para dicho labor, se desarrolló una investigación de carácter descriptivo, así como un método de particularidad inductiva-deductivo.

Terán (2015) en su trabajo denominado "La necesidad de incorporar en el código penal el tipo penal de falsificación informática" aborda como finalidad demostrar la necesidad de la incorporación de la falsificación informática, en la legislación penal boliviana, como nuevo tipo penal. A fin de cumplir los estándares de dicho producto científico, se empleó una investigación de base cualitativa y descriptiva, tomando como muestra la consulta de la doctrina y legislación

comparada vigente de Bolivia y las opiniones de autoridades del órgano judicial respectivo especialmente profesionales abogados.

Ruiz (2016) en su investigación titulada “Análisis de los delitos informáticos y su violación de los derechos constitucionales de los ciudadanos” estipuló como objetivo la aclaración del panorama respecto a los delitos informáticos concretados producto de la violación de los derechos constitucionales de los ciudadanos, en razón de emplear las tecnologías de la información y de la comunicación (TICS), así como de las redes sociales. Por consiguiente, se empleó una investigación de carácter exploratoria, descriptiva y comparativa, en función de un método científico, deductivo, inductivo y sintético para validar los resultados, a partir de una muestra de 30 profesionales en el ejercicio del derecho.

Devia (2016) en su trabajo doctoral denominado “Delito informático: estafa informática del artículo 248.2 del código penal” propugna como meta el otorgar una revisión sintética e integral de los requisitos típicos del delito informático, a fin de materializar una perspectiva idónea y pertinente, respecto de sus antecedentes normativos e implicancias en el mundo jurídico.

**Nacionales**

Morales (2016) en su investigación denominada “La inseguridad al utilizar los servicios de redes sociales y la problemática judicial para regular los delitos informáticos en el Perú-2015” tiene como propósito ilustrar algunas particularidades de los delitos informáticos, para luego realizar algunas críticas respecto a la insuficiencia regulativa en materia digital, respecto a ciertas vulneraciones al derecho a la intimidad. Para dicha meta, se empleó una investigación de carácter descriptiva y comparativa en correlación a una serie de normas como la Constitución Política, la

ley de delitos informáticos, la ley que la modifica, la ley de derechos de autor, el código penal, entre otras.

Alarcón & Barrera (2017) en su estudio científico nominado "Uso de internet y delitos informáticos en los estudiantes de primer semestre de la Universidad Pedagógica y Tecnológica de Colombia, Sede Seccional Sogamoso 2016", tuvo como objetivo principal determinar la relación existente entre el uso del internet y su vertiente de delitos informáticos por los estudiantes de una casa de estudios concreta. Siendo así, la metodología investigativa aplicada cuantitativa de tipo básico, nivel correlacional y diseño no experimental; en adición, se acudió a una muestra de 10 estudiantes para validar las directrices de investigación reseñadas.

Chávez (2018) en su asignación investigativa abordada como "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". En la misma, configuró como objetivo determinar la influencia del delito contra datos y sistemas informáticos en el derecho fundamental a la intimidad personal en la Corte Superior de Justicia de Lima Norte, 2017. Además, se debe precisar que la técnica de investigación se destacó por usar el enfoque cuantitativo, alcance explicativo, diseño no experimental, transversal, correlacional – causal, así como el hecho de que la población fue 510 abogados y la muestra fueron 220 personas. (Chávez, 2018)

En la investigación llamada "Tratamiento jurídico penal de los delitos informáticos contra el patrimonio, Distrito Judicial de Lima, 2018"' denotó como objetivo el análisis del tratamiento jurídico penal de los delitos informáticos contra el patrimonio en el Distrito Judicial de Lima, en el contexto del 2018. Por tanto, se empleó una investigación de particularidad cualitativa y de nivel

descriptivo explicativo. Asimismo, la población y muestra estuvo constituida por duchos e investigadores, tanto nacionales como extranjeros sobre el tema (Pardo, 2018).

Zorrilla (2018) en su investigación nominada como “Inconsistencias y ambigüedades en la ley de delitos informáticos ley nº 30096 y su modificatoria ley nº 30171, que imposibilitan su eficaz cumplimiento” plasmó como propósito el comprobar la presencia de desaciertos entre la ley primigenia que regulaba a los delitos informáticos y su complemento normativo que lo modificó en ciertos artículos, producto de las intenciones del legislador de querer regular los nuevos avances en materia de transgresiones a nivel digital, producto de las novedosas formas de delinquir, partiendo de transacciones, tratos, etc. Así, el tipo de investigación desarrollada fue una de carácter jurídico-dogmático, de diseño no experimental y de corte transversal. Finalmente, la muestra estuvo constituida por 30 jueces, fiscales y otros profesionales de derecho, en el distrito judicial de Huaura.

## Bases teóricas

### Nociones esenciales.

#### *¿Derecho informático o informática jurídica?*

Para iniciar, una de las grandes problemáticas que merece ser atendida, previo a enfocarnos en la especificidad de los delitos informáticos y el gobierno digital, es la discusión entre derecho informático e informática jurídica en razón de que, si bien la primera nominación señalada fue usada en acápites precedentes, se hace indispensable zanjar esta discusión, desde nuestra perspectiva, a fin de aclarar el panorama a desarrollar en los siguientes apartados.

Siendo así, en la literatura especializada pueden ubicarse diferentes posturas al respecto, procediendo a sintetizar algunas de ellas, de la siguiente manera:

Por un lado, de conformidad a Aguilar (2015), se concibe al derecho informático como un agrupamiento de normas jurídicas cuya labor es normar las manifestaciones jurídicas como producto del uso de recursos informáticos por la conducta de particulares sujetos. De esta manera se conciben los efectos de emplear la informática en la vida diaria; verbigracia, conductas de carácter ilícito

Asimismo, en base al referido autor, Aguilar (2015), la noción de informática jurídica puede comprenderse como una disciplina que dispone como propósito que la aplicación de las conocidas tecnologías de la información, producto de la nombrada Ciencia de la Computación, se encuentre factible al marco jurídico a efectos de optimizar y facilitar la labor del Abogado, Jurista y actores de la administración pública y/o judicial.

En otra postura, se considera que derecho informático, en base a Peña (s.f) debe conceptualizarse como una universalidad de problemas materializados en razón de las variaciones acontecidas y desarrolladas por el derecho como resultado de la imperatividad de ciertas actividades pertinentes que se concretan en el contexto social y que necesitan de mejores en sus regulaciones, ya sea a nivel de remodelación total como de una reinterpretación de las regulaciones ya existentes.

En adición a lo anterior, en concordancia al citado autor, Peña (s.f) se ha estipulado que por la idea de informática jurídica debe enfocarse una visión de conceptuar a la relación entre el derecho y las tecnologías de la información, a partir de una primera impresión, es interpretarla

como la concurrencia de las TICS a las actuaciones perpetuadas por quienes actúan en el campo jurídico.

En una tercera mentalidad, se ha expresado que por derecho informático debe suponerse una manera de pensar que la comprenda como un aglutinado de directrices y normas que preceptúan los efectos jurídicos del vínculo entre el Derecho y la Informática. Agregado a ello, es viable considerarlo una temática del derecho especializada en la informática, sus usos, aplicaciones e implicaciones legales. (Canaris, 2015)

A partir de tal concepto, se ha expresado por la misma autora que la distinción con la informática jurídica responde a que esta última se la define como parte de las ciencias de la información cuya esencia es ordenar la concreción de los postulados informáticos en lo jurídico. Siendo así, se expone que la informática jurídica busca estudiar los medios informáticos para fortalecer sus clásicos procesos en el ámbito jurídico: análisis, investigación y gestión. Así, se deja sentado que la misma no constituye una disciplina jurídica, en razón de que su fundamento es esencialmente tecnológico y no jurídico. Asimismo, la autora aclara que la informática jurídica no es parte del Derecho, su temática es fundamentalmente tecnológica y carece de contenido jurídico. Por tanto, se reitera que la misma solo se invoca como una ciencia que involucra el tratamiento lógico e informático de la información jurídica. (Canaris, 2015)

En una cuarta formación de ideas, Malvaez (2008), citando a Pérez, ha comentado que por derecho informático debe entenderse la acepción de conjunto de principios y normas que norman los desprendimientos jurídicos surgidos de la vinculación entre informático y derecho, aunque tampoco visualizan como descabellada una noción que la disponga como conglomerado

de normas jurídicas que regulan los procesos de información, precisándose que lo regulado son las conductas o hechos más que sus efectos.

Igualmente, en base a la cita de Pérez, se ha procedido a plasmar como definición de informática jurídica, al tratamiento uniformizado de las fuentes de conocimiento jurídico (documentación legislativa, jurisprudencial y doctrinal), de funcionamiento jurídico (organismos legislativos y judiciales) y de las resoluciones judiciales (informática jurídica para la toma de decisiones). (Malvaez, 2008)

Por otro lado, en concordancia al pensar de Montaño, Saavedra & Saavedra (2018) y citando estos a Martin & Wilheim, conceptúan al derecho informático como un conjunto de principios y normas que reglan los resultados jurídicos relacionados entre el derecho y la informática. Asimismo, es viable conceptuarlo como una rama del derecho y un marco de desprendimiento del derecho, en obediencia a que los campos del derecho se han avizorado implicancias por la llamada sociedad de la información. Finalmente, también se lo comprende como un agrupado de normas jurídicas que reglan la creación, desarrollo, uso, aplicación de la informática a las disyuntivas materializadas por la misma en donde se presencie un bien que requiera o necesita una tutela jurídica apropiada y responsable.

Adicionado a lo anterior, respecto a la informática jurídica, citándose a Guastavino y Valdez, se ha referido que por dicha figura se entiende una técnica interdisciplinaria cuya finalidad es la operacionalización de la informática a efectos de recuperar data de pertinencia jurídica, así como la producción y aprovechamiento de los instrumentos de análisis y examinación de la aludida información con el propósito de adoptar decisiones con importancia para el marco jurídico. En adición, se dice que esta figura aparece cuando se insertan los

instrumentos informáticos en las particularidades jurídicas indistintas, por lo cual sirve como herramienta técnica que apoyo, auxilia y brinda servicio a diversas actividades del derecho. Por consiguiente, el proceso antes descrito se traduce en materias que pueden resumirse como la ofimática y jurimetría, informática jurídica de gestión, informática jurídica documental, informática jurídica decisional. (Montaño, Saavedra & Saavedra, 2018).

Por consiguiente, sin perjuicio de que los doctrinarios antes citados hayan expuesto sus consideraciones sobre ambas herramientas de forma clara y precisa, es menester explicitar nuestra postura sobre el mismo, así como relacionar ambas figuras a las variables de nuestro estudio, vale recordar, delitos informáticos y gobierno digital, teniendo en cuenta la noción inicial (expuesta en el punto de descripción de la realidad problemática) sobre las mismas.

Así, la informática jurídica se concibe como un conglomerado de mecanismos y/o herramientas, derivadas de las llamadas TICS, a fin de coadyuvar a indistinto operador del derecho (abogado, juez, fiscal u otro símil) al desarrollo de sus labores, teniendo en cuenta que dichas herramientas son producto de la informática per se. Agregado a ello, el derecho informático se puede entender como un marco regulador y director de las hipotéticas consecuencias y efectos, a partir del uso de los mecanismos surgidos producto de la informática stricto sensu, como en el caso de señalar cuando una utilización de una base de datos se configura como conducta legal y cuando es ilegal (en este último supuesto, dictaminando las respectivas sanciones).

Relacionando ambas visiones al tema del gobierno digital y delitos informáticos, diremos que la informática jurídica se aprecia como una herramienta que orienta a un operador del derecho (una entidad de la administración pública) en cuanto a los pasos a seguir para

interrelacionarse de una mejor forma (digitalmente) con el resto de los partícipes de la comunidad, a través de los aludidos proyectos de gobierno digital. De otro lado, el tema del derecho informático se vincula a estipular que los inadecuados manejos de las directrices que componen la implementación de un proyecto de gobierno digital, como el utilizar o sustraer información de una base de datos, pueden acarrear una eventual sanción para el autor de la conducta informática indebida.

### *Las particularidades del avance de la sociedad informática.*

Con relación a este punto, se ha comenzado describiendo la problemática, a partir de las apreciaciones de Bauman, en razón de estar sucediendo una serie transformaciones en lo que se nomina como la sociedad del tercer milenio. Vale decir, se puede observar la transición de una sociedad cuyo margen de actuación se oriente por la estabilidad, la previsibilidad e incluso la repetitividad, a una cuyas particularidades se enfoquen en un ámbio de volubilidad, flexibilidad, así como el que su forma organizativa, de estructuración no se enmarque en un campo de perdurabilidad (Rodriguez, 2013).

Es decir, a decir del mismo autor, nos hallamos en circunstancias en las cuales la citada modernización de la comunidad es vista como algo compulsivo, exasperado, desacatándose ideales de ser una población que participe en una sociedad predecible y estable, permitiendo esta última otorgar un clima aclarador, aunque lento y gradual, para la solventación de los diversos problemas de carácter legal, social, económico y político, siendo dicha solución, como es evidente, de mentalidad permanente, continua, sucesiva en el tiempo (Rodriguez, 2013).

Por lo tanto, en función de los aspectos antes reseñados, es que se aclama la imperiosidad de precisar la noción de sociedad de la información, a partir de lo que el derecho debe regular

como comportamiento, guiándose para ello del profesional especializado en informática. Un dato que no puede obviarse, es que la actualidad nos sumerge en un ámbito que vincula a los estados soberanos a concordar, ante una eventual controversia, sus derechos internos al derecho comunitario como el hecho de que las respectivas resoluciones sean obligatorias para el Estado que forma parte de esa comunidad (Rodriguez, 2013).

Pues bien, retomando el tema de la "sociedad de la información", es importante remitirnos a la denominada "Cumbre Mundial sobre la Sociedad de la Información" y en su "Declaración de Principios", realizada en Ginebra-2003. En la misma se estipula como regla esencial que su edificación integra el reto general del nuevo milenio. Dicho reto implica que su núcleo se caracterice por tener una visión concentrada en la persona, de labor integradora y orientada al desarrollo, y en la cual se pueda consultar, utilizar y compartir la información y el conocimiento para que los diferentes partícipes de la comunidad las utilicen para fortalecer y mejorar el desarrollo sostenible y su calidad de vida (Rodriguez, 2013).

Ahora bien, no está demás tener en consideración que dicha sociedad de la información conlleva un específico grado de desarrollo social, económico y tecnológico, cuyos principales aspectos sean la presencia de diferentes actores nacionales como el gobierno, las empresas, investigadores, centros tecnológicos, organizaciones sociales y ciudadanos, con la mentalidad de materializar la gestión de la información para producir innovadoramente sujeto a los objetivos para el desarrollo" (Valenti, citado en Naser, s.f)

Por último, un relevante dato a tener en cuenta es que gran parte de los Estados Latinoamericanos y Caribeños carecen de un patrón de desarrollo de la Sociedad de la Información integral y debidamente articulado. Dicho sea de paso, los principales aspectos

hechos a un lado pueden resumirse como una falta de ente técnico que lidere y cuente con la capacidad ejecutiva; ausencia de una visión estratégica y programática basada en prioridades; la falta de coordinación entre los sectores público y privado, así como con el académico; ambivalencia innecesaria en las iniciativas, así como la dispersión de esfuerzos y recursos. (Naser, s.f)

## Delitos informáticos

### *Origen del delito informático y curso de acción en la actualidad.*

Para iniciar, es de señalar que los cimientos del delito informático pueden resumirse, de conformidad a Rinaldi (2017) en 3 momentos y de la siguiente manera:

- ✓ En un primer momento, los delitos cibernéticos permitieron que una gran cantidad de fraudes y/o malware se insertaran en el correo electrónico de los usuarios, en el marco de los años 80’.
- ✓ En un segundo instante, durante la época de los años 90’, los delitos cibernéticos procedieron a desarrollarse mediante el avance continuo de los navegadores web. Ello en función de que las variedades de los mismos posibilitaban el surgimiento progresivo de los renombrados virus.
- ✓ En un tercer momento, en el marco de los comienzos del 2000, la siguiente forma de accionar los delitos informáticos fue mediante la operación de las llamadas redes sociales. Es decir, aprovechando que la ciudadanía consignaba la llamada “foto del perfil” se generó una inundación de información personal y un subsecuente incremento de las apropiaciones indebidas de la identidad de una persona (delito informático de suplantación de identidad)

Por consiguiente, a raíz de este breve recuento histórico de los delitos informáticos y de las dificultades afrontadas por las autoridades para poder combatir a los mismos, durante los primeros instantes de su aparición, es que se puede describir un aglutinamiento de mecanismos que han permitido iniciar las primeras y actuales acciones de combate a dicho delitos informáticos o cibernéticos, resumiéndolas así:

- ✓ Dación de leyes de delitos informáticos por cada país concreto
- ✓ Emisión e incorporación de directrices específicas, en materia de delitos informáticos, en los corpus penales de los diversos Estados.
- ✓ Concreción de conversatorios y diálogos para abordar las fortalezas, oportunidades, amenazas y debilidades, en cuanto a las medidas implementadas para combatir los delitos informáticos.
- ✓ Emisión de tratados internacionales y recomendaciones por las Naciones Unidas, en materia de delitos informáticos.
- ✓ Estudios científicos por parte de diversos doctrinarios en materia de delitos informáticos.
- ✓ Entre otras acciones particulares de cada país.

### *Concepción de delito informático.*

Por un lado, se ha definido que por delito informático se vincula una idea de concretar un crimen mediante el empleo de una serie de instrumentos informáticos, llámese computadora, internet, entre otros. Además, también se ha dejado en claro que tal forma de criminalidad no siempre se finaliza por tales medios, ya que existen casos donde facilitará la dación de tales crímenes, más no determinan su respectiva perpetuación. Si bien puede ser cierto que denominación (delitos informáticos) no es empleada frecuentemente en los marcos normativos

penales, la misma colabora para identificar, estudiar y sancionar un nuevo método de criminalidad, en este caso, bajo la tecnología informática. (Mazuelos, citado en Villavicencio, 2014).

Después, el delito informático se lo ha concebido como un acto donde se involucra un sistema tecnológico (computadora), el cual se emplea como un instrumento que propicie el desarrollo de un hecho criminológico, el cual no tiene otro fin que atentar contra derechos, garantías y libertades comunitarias. (Estrada & Somellera, 1998).

De otro lado, se ha referido que por delito informático debe definirse un aglutinado de diligencias criminales que las diversas legislaciones penales, a nivel internacional, han tratado de encajar en un genérico tipo penal; ejemplo de ello sería encuadrarlo como agravante o medio de comisión de un fraude, robo, hurto, estafa, entre otros. Sin embargo, se pone en conocimiento que la regulación del derecho, de esta figura, devino en obligatoria en razón del frecuente manejo inadecuado de las computadoras u otras técnicas informáticas. (Delgado, 2014).

Aparte, se ha dicho que delito informático importa toda acción con intencionalidad, actitud de provocar un daño, perjuicio o menoscabo a una persona natural o jurídica, aunque dicho comportamiento doloso no siempre genere un beneficio material para el actor del delito o aun cuando no dañe de manera directa al afectado y en cuya realización se empleen dispositivos ubicados en el campo de las llamadas actividades informáticas. (Camacho, citado en Loredo & Ramírez, 2013)

En otro orden de términos, se ha manifestado que por delito informático se concibe todo accionar ilícito (y, por ende, proscrito y sancionado por las normas del campo penal) concretado mediante el empleo de medios informáticos (producidos por la aparición de las nuevas tecnologías), sea para materializar el delito propiamente dicho o como un mecanismo que propicie su

perpetuación, derivando dichos accionares a una afectación de los datos abarcados en un sistema. (Viega, 2011)

Asimismo, en un enfoque más crítico, se ha referido que ciertos pensamientos de los juristas especializados en el derecho han dejado sentado que el delito informático alude a una metodología única de concreción; sin embargo, dicha idea es errónea, en razón de que el delito informático como tal denota una modalidad plural de comisión, ya que se alude una variedad de conductas ilícitas y no un comportamiento general. Siendo aún más específico, el delito informático per se puede construirse a partir de una de tantas modalidades que pueda hablarse, de conformidad al marco normativo concreto. (Casabona, citado en Acurio, 2015).

De todo lo anterior, se ha dejado en claro de que si bien los delitos informáticos pueden enfocarse de distintas maneras y variada terminología, según el autor específico, lo cierto es que la esencia del concepto, a partir de concordar todas las acepciones antes mencionadas, reside en que el delito informático busca generar un perjuicio a un actor concreto y su sistema de datos, mediante las tratativas de una serie de acciones que se valen de los indistintos medios provistos por las referidas tecnologías de la información.

### *Sujetos de los delitos informáticos.*

A manera de introducción, puede manifestarse que las particularidades que constituyen al llamado ciberdelincuente o sujeto activo del delito informático, son diversas, pudiendo sintetizarlas como estas: Disponer un de un avanzado dominio en materia de sistemas informáticos, contar con un puesto estratégico en su lugar de labores, en los cuales se estudia y conserva información y/o documentación de carácter confidencial-relevante, sea para la institución como para la población (por este acto, se ha llegado a calificar dichos actos como delitos ocupacionales). Agregado a ello,

se ha referido que este los actos elaborados por el ciberdelincuente ingresan en un ámbito de "delitos de cuellos blancos" (Azaola, 2010).

En otro parecer, se ha mencionado que por sujeto activo puede comprenderse a cualquier persona si y solo si el mismo tenga a su disposición una agrupación. Respecto a si es indispensable que se cuente con un puesto laboral en la institución donde se afectará la base de datos, se ha dicho que tal carácter no necesariamente es esencial para la materialización del delito, pero ello no quiere decir, claro está, que se excluya a aquellos actores con una posición estratégica que les permita desarrollar la conducta ilícita. En razón de ello, al sujeto activo se lo comprende en 2 vertientes: Por un lado, los hackers son personas orientadas a vulnerar programas y sistemas informáticos cuya motivación es la cotidianeidad, la diversión u otro tipo de interés. De otro lado, están los crackers, siendo aquellos sujetos que operan en los sistemas de las entidades con el propósito de generar problemáticas a los mismos, mediante diferentes móviles. Ejemplo de ello puede ser la destrucción de datos o impedimento de acceso al usuario. Es de referir que a los crackers también se los suele calificar como piratas electrónicos (Villavicencio, 2014).

Un dato a precisar, en el ordenamiento jurídico peruano, es el hecho de que al seguir vigente el latinismo "societas delinquere non potest" no es factible encuadrar en el calificativo de sujeto activo, a la persona jurídica. Sin perjuicio de ello, no debe olvidarse que el derecho penal nacional norma un modelo conocido como consecuencias accesorias, en caso los representantes de una entidad cometan un delito informático. Ahora bien, la figura es distinta, si pensamos en calificar a la persona jurídica, en sus diferentes calidades (públicas y/o privadas) como sujeto pasivo (Villavicencio, 2014).

Por otra parte, se ha referido que por sujeto pasivo y/o víctima, por excelencia, es la persona jurídica, en razón estar inmersa en el tráfico económico donde se realizan sus actividades. Ejemplos de dichos sujetos pasivos son diversos, entre otros: La banca, las instituciones públicas, la industria de transformación, etc. (Gutiérrez, 1991).

Agregado a ello, se ha manifestado por sujeto activo de un delito informático o cibernético puede entenderse 2 perspectivas: Un ducho en la materia informática y otro que no pero con un mínimo conocer de la temática aludida. A raíz de ello, se ha generado una disyuntiva producto del concepto de "niños genio", debido a que los mismos en base a su conocimiento, pueden elaborar y desarrollar las estrategias necesarias a efectos de intervenir en los sistemas informáticos objeto de vulneración, sea de nivel básico o incluso avanzados, lo cual acarrea serios problemas en el tema de delimitar la punibilidad del hecho, ya que es de recordar que los mismos no responden penalmente, por regla general (Delgado.2014).

En otro campo, se ha dicho que el calificativo de delincuente, en esta tipología de delitos, no le corresponde a cualquier actor, sino que la misma se encuentra en dependencia a cumplir una serie de requisitos como el poseer importantes conocimientos de informática; ocupar una posición que le facilite la labor informática delictiva, en su centro de labores; el análisis, en función del caso concreto, respecto a si es o no un factor indispensable el tema educacional en materia informática, para la comisión del delito, es decir, que opere como un indicio en la investigación del hecho punible; estar caracterizado de cierto status económico, lo cual ha derivado en considerarlo como un delito de "cuello blanco. Mientras que, por sujeto pasivo, se ha dicho que es un ente afecto a la acción u omisión perpetrada por el sujeto activo del delito cibernético (Viega, 2011).

Aparte de ello, se ha dicho que sujeto activo es aquel actor que tiene a su merced un conglomerado de habilidades en la utilización de herramientas informáticas los cuales pueden, para concretar su actuar ilícito, contar con un lugar estratégico por su marco laboral (insiders), o en su defecto, manejar dichas habilidades en sistemas computarizados aun cuando no tienen una posición estratégica en dicha empresa, para el desarrollo del delito informático (otusiders). En cambio, por sujeto agraviado de dicho delito se ha vertido que el mismo es todo aquel actor que sufre el accionar o dejar de accionar del delincuente cibernético, volviéndose a recalcar que el victimario puede clasificarse en individuos, instituciones crediticias, gobiernos u otro agente que utiliza sistemas automatizados de información (Acurio, 2015).

En síntesis, en función de cada idea expuesta en las líneas de esta sección, se puede concluir que el sujeto activo del delito informático puede contar tanto con un sofisticado grupo de conocimiento en materia informática como un de un aglutinado mínimo pero suficiente, para su actuar delictivo. A ello se suma, que el sujeto pasivo o victimario del delito informático es aquel individuo o persona jurídica (aunque es más frecuente que lo sea este último) que sufre el menoscabo a su respectivo sistema de datos, computarizados y/o tecnológicos, producto de los medios comisivos empleados por el delincuente cibernético.

### *Bien jurídico tutelado.*

Respecto a este punto, se puede decir que determinado sector de la doctrina especializada en materia de delitos informáticos y concordando dichos conocimientos con los parámetros dispuestos por las respectivas legislaciones penales, ha señalado que el bien jurídico a salvaguardar por las normas en materia de delitos informáticos es el valor patrimonial que tienen los bienes informáticos como: el dato, la información, el programa y el sistema informático. A pesar de ello,

se considera que dicha incursión por delimitar el bien jurídico protegido es precipitada, ya que la configuración del interés jurídico defendido requiere una predominancia del texto normativo sobre el título (sección o capítulo), en base a que el mismo es más vinculante y de mayor riqueza descriptiva. Por tanto, se ha apuntado que el bien jurídico que se protege frente a los delitos informáticos no se circunscribe a un ámbito patrimonial del propietario de los sistemas informáticos dañados, este último se califica más como un bien jurídico secundario; sino a la integridad y disponibilidad que puedan tener los datos y sistemas informáticos (Salvadori, 2013).

Fortaleciendo lo previo, se ha dicho que el bien jurídico en el delito informático puede concebirse desde 2 perspectivas: La general, en la cual se ubica a la información contenida, estudiada y transmitida a través de diferentes mecanismos de tratamiento automatizado de datos. Segundo, la residual, en la cual se comprenden el resto de bienes transgredidos por las modalidades de los delitos informáticos, como el caso de la indemnidad sexual, intimidad u otros (Villavicencio, 2014).

### *Delitos informáticos en la legislación nacional.*

Con regulación al margen de normar los delitos informáticos en la legislación peruana, puede decirse que los mismos han sido divididos en una clasificación que puede resumirse como la siguiente:

1. “Delitos contra datos y sistemas informáticos”
2. “Delitos contra la indemnidad y libertad sexual”
3. “Delitos contra la intimidad y el secreto de las comunicaciones”
4. “Delitos contra el patrimonio”
5. “Delitos contra la fe pública”

6. Delitos informáticos abarcados en disposiciones genéricas

Al margen de haber descrito dicha clasificación, para los propósitos de la presente investigación nos delimitaremos a exponer y analizar los tipos penales respecto a los puntos 1, 4 y 5. Aunado a ello, se debe dejar en claro que la esencia del presente trabajo conllevará a examinar las conductas criminosas *per se*, haciendo a un lado el tema de las penas (cárcel, prestación de servicios comunitarios, etc.) aunque no por ello queremos decir que las mismas son irrelevantes para todo estudioso de la materia de delitos informáticos.

En un primer orden de términos, es de precisar que, en los delitos informáticos contra datos y sistemas informáticos, pueden ubicarse 3 tipos penales: Acceso ilícito (art.2) y atentado a la integridad de los datos informáticos, mediante 2 modalidades este último (art.3 y 4), a pesar de que sus 2 formas de materialización las concibe la Ley N° 30096 (2013) y su modificatoria, la Ley N° 30171 (2019), como independientes.

Con relación al delito de "acceso ilícito", la norma en mención regula lo siguiente: "El que deliberada e ilegítimamente accede a todo o en parte de un sistema informático, siempre que se realice con vulneración de medidas de seguridad establecidas para impedirlo (…)".

Como se puede observar, el tipo penal de acceso ilícito dispone la penalidad de aquellas conductas que con deliberación (intencionalidad, dolo) y de forma ilegítima (sin autorización) buscan acceder, ingresar, sea de forma total o parcial, a un determinado aparato informático. La redacción de este punto de la norma no contrae mayores ambigüedades para un ávido lector de la normativa; sin embargo, consideramos que la continuación del tenor de la norma es una redundancia de la terminología "ingreso ilegítimo", ya que es evidente que todo ingreso sin autorización a un sistema informático tuvo que materializarse a partir de sobrepasar los protocolos

de seguridad destinados a evitar, justamente, dichos ingresos ilegítimos. Al margen de dicha observación, no se presente mayor problema en este supuesto penal.

Respecto al tipo penal de atentado a la integridad de los datos informáticos, en su primera vertiente, la Ley N° 30096 (2013) y su modificatoria, la Ley N° 30171 (2019), dispone que: "El que deliberada e ilegítimamente daña, introduce, borra, deteriora, altera, suprime o hace inaccesibles datos informáticos (…)".

Al igual que el anterior supuesto comentado, este tipo penal manifiesta una intencionalidad (ánimo de ocasionar un menoscabo) así como un accionar carente de permisibilidad, mediante el cual se desarrollan una serie de conductas por acción como: ingresar, eliminar, dañar, alterar, suprimir, como por omisión o hacer inaccesible, mediante las cuales se afectan datos informáticos.

Sobre el tipo penal de atentado a la integridad de los sistemas informáticos, la Ley N° 30096 (2013) y su modificatoria, la Ley N° 30171 (2019), enfatiza que: "El que deliberada e ilegítimamente inutiliza, total o parcialmente, un sistema informático, impide el acceso a este, entorpece o imposibilita su funcionamiento o la prestación de sus servicios (…)".

Haciendo mención a sus particularidades de esta segunda modalidad de atentar contra la universalidad del conglomerado informático, en este caso, de los sistemas informáticos, se vuelve a reiterar el tema de intencionalidad (no ingresa el tema de la culpa) y desarrollo de la acción sin permiso alguno. Asimismo, la diferencia de esta segunda modalidad estriba en que mientras el anterior artículo sancionaba un comportamiento que afectara a la unidad de dicho conglomerado informático, lo que se sanciona aquí es que se impida que, a partir de dicho conglomerado informático, se concreten sus finalidades específicas, como servir para prestar un servicio a la población, etc.

En un segundo lugar de términos, con referencia a los delitos informáticos contra el patrimonio, es de poner en conocimiento que la única figura que contempla dicha sección es el llamado fraude informático (art. 8). Por ende, esta figura, de conformidad a la Ley N° 30096 (2013) y su modificatoria, la Ley N° 30171 (2019), estipula que:

> El que deliberada e ilegítimamente procura para sí o para otro un provecho ilícito en perjuicio de tercero mediante el diseño, introducción, alteración, borrado, supresión, clonación de datos informáticos o cualquier interferencia o manipulación en el funcionamiento de un sistema informático (…) (Ley N° 30171, 2019).

En cuanto a la figura del fraude informático, es posible ver que sus especificidades nos conllevan a enmarcar nuestro rango de observancia en un más allá del tipo penal de acceso ilícito a los datos informáticos, ya que mientras este último desarrollaba una conducta de un simple ingreso desautorizado a la base de datos informáticos (y lo que derivaba a la pertinente pena), el fraude informático no se completa con el solo ingreso con dolo y sin autorización sino, además, requiere la dación de un beneficio personal para el autor del ilícito, o en su defecto, para un tercero (sin importar el medio comisivo a emplear para concretar el hecho punible). Como puede verse, el elemento determinante del fraude informático es el surgimiento de un provecho indebido, a partir del acceso informático sin la venia requerida. Aun así, un aspecto que no puede dejarse de lado, en referencia al provecho para tercero, es que este último debe tener una vinculación con el autor del delito, ya que en caso de no tenerla y verse beneficiado, consideramos que el mismo debe poner en aviso a la autoridad respectiva del provecho recibido de forma incorrecta, a efectos de encontrarse exento de algún tipo de pena, ya que de lo contrario se asumirá que dicho funcionario sí se ubica en algún tipo de relación, vinculación con el delincuente y, en consecuencia, procedería la respectiva sanción.

En un tercer marco de palabras, respecto a los llamados delitos informáticos contra la fe pública, la figura que se contempla por la Ley N°30096 y su modificatoria, la Ley N° 30171 (2019), es la denominada suplantación de identidad (art. 9), conceptuada en los siguientes términos: “El que, mediante las tecnologías de la información o de la comunicación suplanta la identidad de una persona natural o jurídica, siempre que de dicha conducta resulte algún perjuicio, material o moral (…)”.

Como puede desprenderse de los detalles acotados por el artículo citado, se tiene que aquí no se alude a un mero ingreso indebido o un provecho inadecuado, sino que el comportamiento reprimido se describe como la sustitución de identidad de una persona natural o jurídica, mediante los mecanismos tecnológicos en su innumerable clasificación. Un primer detalle a rescatar es que el legislador no hace mención expresa de la deliberación e ingreso ilegítimo, como en los artículos anteriores, más dichos aspectos pueden deducirse en función de la gravedad de una conducta, como lo es el propósito delineado de suplantación. Asimismo, puede comprenderse que el suplantado puede ser tanto un agente del sector público como un usuario al cual esté registrado en la base datos (como aquel que tiene en curso un trámite). Sin embargo, lo que consideramos como controvertido es condicionar la punibilidad del hecho a que de su dación se genere un daño material, moral o perjuicio de cualquier clase, cuando, en realidad, la sola falsedad y/o adulteración de la imagen de una persona, a través de medios informáticos, constituye una actuación incompatible con las directrices del ordenamiento jurídico. Aclararemos esto con un ejemplo: Supongamos que X, el infractor, ingresa ilegítimamente a la cuenta de funcionario Y, de la entidad pública Z. En un primer momento, lo que realiza X es utilizar la cuenta de Y para alterar ciertas páginas de la institución, con el objeto de atribuirle una buena práctica y, como resultado, se le otorgue un reconocimiento desmerecido. Si bien este caso puede sonar extravagante, el propósito es ir hasta el extremo para

compartir cuan controversial es la literalidad de la norma. En un segundo momento, lo que desarrolla X ahora, mediante los medios tecnológicos a su disposición, es emplear la cuenta de Y para suprimir información que pudiera comprometerlo con algún tipo de delito. Como es evidente, al identificarse dicha supresión, la institución sufrirá un menoscabo al ver su imagen pública cuestionada, por lo que optará por sancionar con la suspensión y/o cese al respectivo funcionario que borró dicha información de relevancia pública, aun cuando este no perpetuó tal ilícito. La incógnita que aparece es ¿Solo en este último supuesto se debe penalizar al infractor, X? La solución de dicho dilema es negativa, a nuestro parecer.

### *Delitos informáticos en la legislación comparada.*

Con relación al marco normativo comparado y/o extranjero, respecto a los delitos informáticos, nos avocaremos a estudiar 4 sistemas reguladores (Argentina, Colombia, España e Italia) de conductas informáticas ilícitas, específicamente, aquellas relacionadas al propósito de nuestro tema de investigación.

En primer lugar, con relación al campo español, de conformidad a su Código Penal (1995), tenemos 2 artículos específicos a analizar.

Por un lado, tenemos al artículo 278 del referido Código Penal de España (1995), el cual estipula que:

> El que, para descubrir un secreto de empresa se apoderare por cualquier medio de datos, documentos escritos o electrónicos, soportes informáticos u otros objetos que se refieran al mismo (…) si se difundieren, revelaren o cedieren a terceros los secretos descubiertos (…) (Código Penal de España, 1995).

Como es de observar en el artículo in comento, la conducta sancionada por el margen jurídico español está referido a la intencionalidad (dolo) del sujeto activo en torno al apoderamiento de una estructura informatizada digitalizada, sea mediante herramientas escritas o tecnológicas, con el único propósito de acceder a descubrir aspectos confidenciales de una empresa en específico (sujeto pasivo). De conformidad a las particularidades de este tipo penal, podemos asemejar este supuesto al hecho punible "acceso ilícito", tipificado por nuestra normativa penal, ya que lo tratado es un acceso ilegítimo y deliberado (es claro que el autor del delito tiene que valerse de medios alternativos-punibles para acceder a información privilegiada de la entidad conculcada)

Aparte, se tiene el artículo 536 del ya mencionado Código Penal de España (1995), el cual plasma que:

> La autoridad, funcionario público o agente de éstos que, mediando causa por delito, interceptare las telecomunicaciones o utilizare artificios técnicos de escuchas, transmisión, grabación o reproducción del sonido, de la imagen o de cualquier otra señal de comunicación, con violación de las garantías constitucionales o legales (…) (Código Penal de España, 1995).

Si bien es cierto que esta conducta podría encajar en un tipo penal de vulneración a la privacidad de las comunicaciones (conducta que no fue abordada, para los propósitos de este estudio, aunque hemos señalado su acogimiento expreso como delito informático), la importancia que le otorgamos a este comportamiento punible se encuentra en función de la calidad del agente que perpetua la conducta contraventora del ordenamiento, ya que se alude de forma explícita al actor público, sin importar su modalidad específica (tener presente que, en

nuestro país, se considera funcionario agente público al trabajador con cargo de confianza en la administración pública y aquel que carece de dicha confianza, encaja en el llamado servidor público). Verbigracia, si es un funcionario de una institución pública quien intercepta una comunicación (por ejemplo, una que pudiera derivar al inicio de un procedimiento administrativo sancionar en su contra e, incluso, una eventual investigación penal), es claro que incurre en este tipo de delito informático.

En segundo lugar, con referencia al campo jurídico de Argentina (1921) y su reforma producto de la Ley 26.388 (2008) contemplan una serie de articulados, sobre delitos informáticos, que procedemos a estudiar.

En cuanto al artículo 157 de dicho Código Penal de Argentina (1921) y su reforma producto de la Ley 26.388 (2008), se tiene que:

> Será reprimido (…) el que: 1. A sabiendas e ilegítimamente, o violando sistemas de confidencialidad y seguridad de datos, accediere, de cualquier forma, a un banco de datos personales; 2. Ilegítimamente proporcionare o revelare a otro información registrada en un archivo o en un banco de datos personales cuyo secreto estuviere obligado a preservar por disposición de la ley. 3. Ilegítimamente insertare o hiciere insertar datos en un archivo de datos personales (Código Penal de Argentina, 1921).

Como puede verse de las 3 conductas que regula este artículo, es factible observar una conjugación de los tipos penales informáticos peruanos en materia de acceso ilícito, atentado contra la integridad de datos informáticos y de fraude informático. Esta apreciación obedece a que este artículo del código penal argentino, en un instante, condena el mero acto de ingresar a un conglomerado de almacenamiento digital de una entidad específica (acceso ilícito). Asimismo, la

similitud con el delito de fraude informático nacional se puede deducir de la terminología que desprende el traslado de la información confidencial de la empresa a un tercero, ya que no es descabellado razonar que el susodicho traspaso de información propicie algún beneficio para el tercero receptor de la información reservada de la persona jurídica. Finalmente, el tema de la presencia del atentado contra la integridad de datos informáticos se observa en este artículo a partir de su modalidad de concreción "alterar una base de datos ilegítimamente", ya que el accionar de insertar datos en un sistema de tecnología de datos (marco argentino), sin permiso alguno, encaja en el comportamiento citado de alterar.

Además, con referencia al inciso 16 del artículo 173 de dicho Código Penal de Argentina (1921) y su reforma producto de la Ley 26.388 (2008), se puede observar que: "El que defraudare a otro mediante cualquier técnica de manipulación informática que altere el normal funcionamiento de un sistema informático o la transmisión de datos (…)".

Acerca de este artículo, es de manifestar que, a nuestro juicio, esta modalidad penal argentina de delitos informáticos se considera como una forma de materializar un atentado contra la integridad de sistemas informáticos, no acogida por la legislación peruana. Nos explicamos. El atentado a la unidad de los sistemas informáticos en materia peruana hace mención a un ingreso deliberado e ilegítimo, pero en el contexto argentino nos encontramos ante un ingreso legítimo al sistema de información digital (producto de un convenio con un tercero con dominio de la temática informática). Por consiguiente, el hecho punible en que incurre el actor del delito, para el caso argentino, es atentar contra la unidad de sistemas informáticos de una entidad, valiéndose de la confianza depositada por un representante de la persona jurídica afectada.

Asimismo, acerca del artículo 183 del mencionado Código Penal de Argentina (1921) y su reforma producto de la Ley 26.388 (2008), se dispone como conducta punible: “El que alterare, destruyere o inutilizare datos, documentos, programas o sistemas informáticos; o vendiere, distribuyere, hiciere circular o introdujere en un sistema informático, cualquier programa destinado a causar daños (…)”.

En función de las particularidades de este tipo penal, es de señalar que el accionar sancionado por este artículo y que merece comentario es lo relativo a comercializar la inserción y/o disposición de un medio informático, sin atender a su naturaleza, con orientación a propiciar un menoscabo, perjuicio, en razón de que la primera parte de este artículo es una sencilla redundancia del delito de transgredir la uniformidad del sistema digitalizado de información. Pues bien, consideramos que el propósito legislativo es idóneo, ya que busca penar cualquier clase de daño producido a un sujeto mediante el empleo de cualquier instrumento de carácter informático, producto de su previa transferencia, cesión u otra forma de traspaso del dominio de dicho medio informático. En todo caso, respecto a la redundancia manifestada, creemos que la lectura correcta del artículo debe ser el atentado contra la integridad de los datos y/o sistemas informáticos, producto de una previa comercialización de la herramienta informática a emplear, y con propósitos de generar un daño concreto, sea cual sea la alícuota del mismo.

En un campo aparte, en concordancia al artículo 255 del aludido Código Penal de Argentina (1921) y su reforma producto de la Ley 26.388 (2008), se abarca la siguiente ilicitud:

> Será reprimido (…) el que sustrajere, alterare, ocultare, destruyere o inutilizare en todo o en parte objetos destinados a servir de prueba ante la autoridad competente, registros

> o documentos confiados a la custodia de un funcionario público o de otra persona en el interés del servicio público (…) (Código Penal de Argentina, 1921).

Queremos detenernos en este artículo, ya que el léxico empleado por el mismo nos da visos para entender por qué calificamos a las particularidades del suceso acontecido en OSITRAN, respecto a una presunta supresión de información de relevancia pública y comprometedora de ex-actores del servicio público, como un delito informático. Para aclarar el panorama señalado, procedemos a encajar el supuesto de hecho y consecuencia de este artículo con lo acontecido en OSITRAN: Si un sujeto X (puede ser el ex funcionario de OSITRAN o un tercero por su encargo) destruye información de relevancia pública, de interés al servicio público (caso Chinchero y que denota responsabilidad penal para dicho ex-agente de OSITRAN), es claro que dicho sujeto transgresor de la norma debe ser reprimido. Como es de verse, si bien lo ocurrido en OSITRAN aún se encuentra en investigación, suponiendo que sea verídico, dicho accionar inadecuado sí puede encajar en un delito informático, aunque en concordancia al margen jurídico argentino.

En un tercer momento, analizando los parámetros del Código Penal de Italia (1930), se tiene que las conductas pertinentes para nuestro estudio, en materia de delitos informáticos, se desglosan a partir de su artículo 635.

Por un lado, se tiene el llamado delito de daños a la información, datos y programas informáticos, sancionado por el artículo 635-bis del Código Penal de Italia (1930), penalizando dicha regla a quien: “(…) Destruyere, deteriorase, borrase, alterase o suprimiese informaciones, datos o programas informáticos ajenos (…)”.

Como es observar, se puede destacar que la conducta sancionada por este parágrafo del código penal italiano constituye un reiterar del aludido delito de atentado contra la integridad de la

información digital de una corporación, en su primera modalidad del marco jurídico peruano (datos informáticos), motivo por el cual no se efectuarán mayores comentarios al respecto.

De otro lado, se dispone del llamado delito de daños a sistemas informáticos y telemático, conforme al artículo 635-quater del Código Penal de Italia (1930), disponiéndose que se castigue a quien:

> Mediante las conductas mencionadas en el artículo 635-bis o a través de la introducción o la transmisión de datos, informaciones o programas informáticos destruya, dañe o inutilice en todo o en parte sistemas informáticos o telemáticos ajenos, u obstaculice de manera grave su funcionamiento (…) (Código Penal de Italia, 1930).

Como se puede visualizar, el accionar penado por este artículo del código penal italiano constituye una reincidencia del aludido delito de atentado contra la integridad de la información digital de una corporación, en su segunda modalidad del marco jurídico peruano (sistemas informáticos), también concebido y explicado en la parte argentina de delitos informáticos.

A un lado de lo anterior, se tiene a una tercera conducta ilícita denominada daños a datos y a sistemas informáticos de utilidad pública, sancionada por el artículo 635-ter del Código Penal de Italia (1930), disponiéndose la represión a quien se encarga de: "(…) Destruir, deteriorar, borrar, alterar o suprimir informaciones, datos o programas informáticos de relevancia pública".

Una vez más, nos parece interesante el hecho de que la legislación italiana conciba el tipo penal en el cual encajan los hechos constituyentes del dilema que cuestiona la legitimidad del proyecto digital del OSITRAN, como bien se explicó al tratarlo en el caso argentino. Al margen de no hacer un mayor énfasis en nuestros comentarios, solo queremos dejar resaltado

un llamado de atención para el legislador peruano en torno al por qué no reguló taxativamente esta figura de delito informático, la cual podría propiciar un mayor avance en las investigaciones de responsabilidades respectivas.

En un cuarto momento, respecto al campo colombiano, consideramos explicativo y fructífero, para la esencia del trabajo, la explicación de los principales tipos penales informáticos, razón por la cual procedemos a compartirlo:

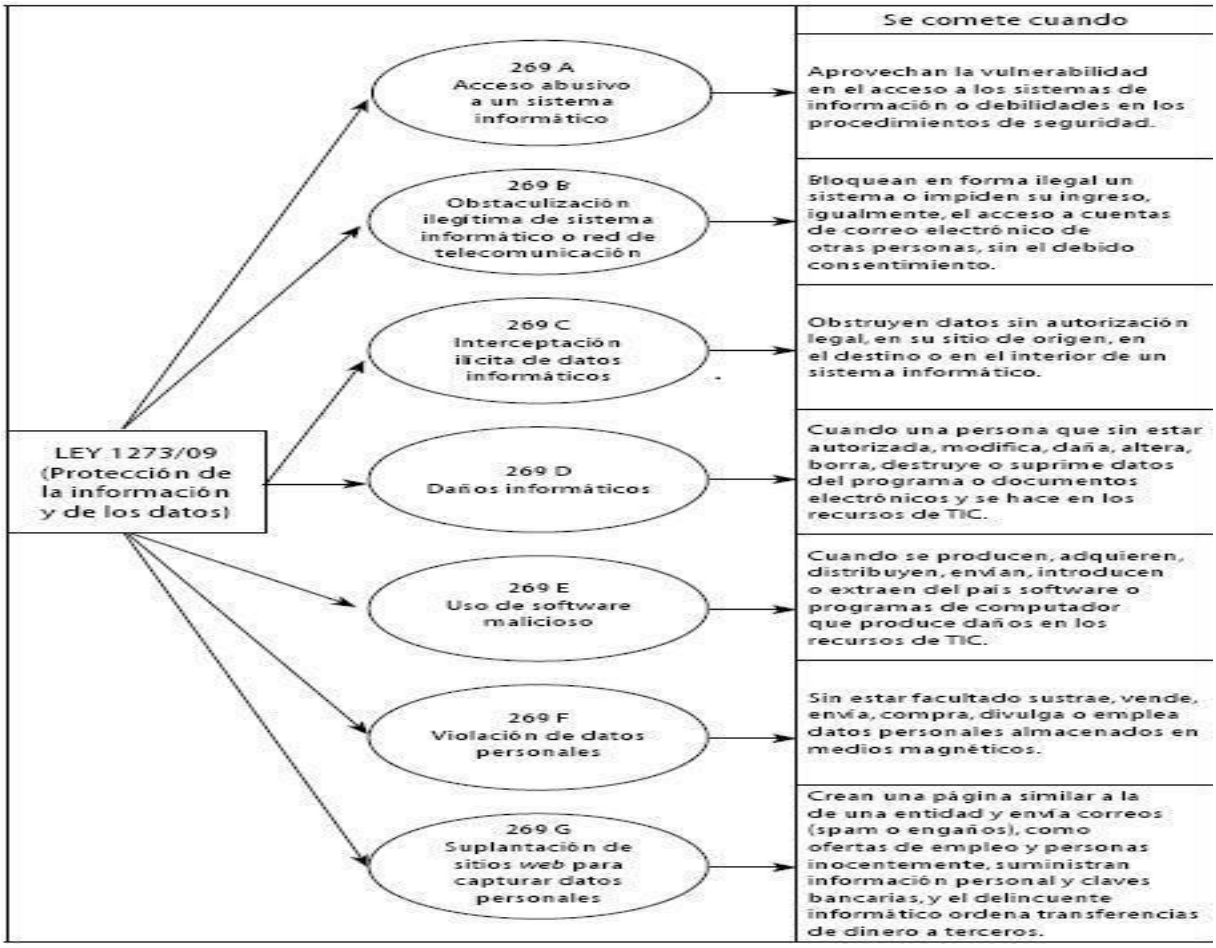



***Figura 1:*** **Tipos penales informáticos en el campo colombiano.**
**Fuente**: Arias-Flórez Daza-Martínez, Ojeda-Pérez y Rincón-Rodríguez (2010)

### *Delitos informáticos en la legislación supranacional.*

A efectos de abordar el marco supranacional o internacional, para el caso de los citados delitos informáticos, es de señalar que el instrumento esencial en la materia es el llamado "Convenio sobre la Cibercriminalidad o Convenio de Budapest" (2001). Este instrumento internacional, desde su entrada en vigencia en 2004, ha sido suscrito y ratificado por diversos Estados de la comunidad europea y latinaomericana. Por citar algunos ejemplos, puede mencionarse al Perú como a los países del marco comparado estudiado (Argentina, Colombia, España e Italia).

Siendo así, es de señalar que el Perú, a efectos de construir su normativa en el ámbito de delitos informáticos, se apegó en una gran proporción a dicho documento internacional, al igual que los otros países pertenecientes a este convenio. Sin embargo, dicho seguimiento interno no se ciñó a una disposición que sí fue concebida en los sistemas extranjeros estudiados. Nos referimos, claro está, al deber de conservar información, por parte de la entidad a través de indistintos actores, cuando la misma es imprescindible para fines de interés público y el cómo se sanciona cualquier conducta destinada a modificarla, alterarla, suprimirla u otro acto de semejante esencia delictiva. Por consiguiente, empezaremos tocando aquellos fenómenos delictivos-informáticos comprendidos por el Perú, para luego explicar aquellos no regulados y que, a nuestro juicio, deberían haberse normado.

Sin perjuicio de lo anterior, el Convenio de Budapest (2001) dispone que ciertas conductas calificadas como "delitos informáticos" deben ser estudiados y aplicados por el legislador de cada país, en función de las particularidades de sus debidos ordenamientos jurídicos:

Por ejemplo, en el artículo 2 de dicho Convenio Internacional, se hace mención al connotado “acceso ilícito”, del cual se deriva un mandato a los Estados Partes de identificar y materializar las medidas pertinentes que crean convenientes con el objetivo de tipificar aquel accionar que implique una inserción ilegítima y deliberada, sea parcial o total, a un sistema informático. Incluso, dicho párrafo del convenio amplía su visión al conceder la potestad a los Estados de determinar si para la comisión del ilícito se requiere vulnerar medidas de seguridad o que el medio informático empleado se encuentre vinculado a otro de parecida naturaleza. A nuestro pensar, es claro que todo ingreso ilegítimo suele producirse, en la mayoría de los casos, vulnerando las medidas de seguridad respectivas. No obstante, ello es claro que el legislador buscaba, conforme puede deducirse, ser más taxativo en el tema, por lo que siguió en dicho aspecto a las líneas que fundamentan el artículo 2 del Convenio de Budapest. Situación distinta se visualiza para el tema de condicionar la comisión del ilícito a una conexión con otro sistema informático, al no contemplarse dicha modalidad en el “acceso ilícito informático”, en el caso del Perú.

Respecto al artículo 4 del Convenio, es de observar que el mismo constituye la esencia de la primera modalidad del atentando a la unidad de los medios informáticos, en este caso, para el caso de los datos informáticos, el cual, rememorando, se producía sea por un daño modificación alteración, supresión de los mismos, así como estando condicionado, siempre, a un ingreso ilegítimo y deliberado. Una salvedad de este artículo que realizó el instrumento internacional es dejar al arbitrio de cada Estado, el que la punibilidad del hecho requiera un daño grave, lo cual no fue contemplado en nuestro marco legislativo de delitos informáticos.

Con relación al artículo 5 del Convenio, es de observar que el mismo constituye la esencia de la segunda modalidad del atentando a la unidad de los medios informáticos, en este caso, para el tema de los sistemas informáticos, el cual, recordando, se producía sea por un daño modificación

alteración, supresión de los mismos, así como estando condicionado, siempre, a un ingreso ilegítimo y deliberado.

Con relación al artículo 8, que concibe el llamado Fraude informático, es de observar que la transcripción de esta modalidad de delito informático ha sido tratada, como tal, en la legislación peruana. Es decir, los elementos configurantes de accionamiento con intencionalidad e ilegitimidad a través de un mecanismo digital con el propósito de alterar, borrar o suprimir datos informáticos, con la intención, así como el concretar dichas conductas sobre un sistema informático con la finalidad única y exclusiva de edificar un beneficio personal o para un tercero, han sido expresados en los vocablos nacionales que atañen a esta figura del fraude informático.

Hasta aquí, se ha abordado lo concerniente a los delitos informáticos regulados por el nivel nacional, en concordancia a los lineamientos del Convenio de Budapest. Como bien se señaló, el tema de las conductas respecto a la intercepción de datos informáticos, vulneración a la intimidad y/o pornografía infantil también han sido acogidas por el referido instrumento internacional y nuestro ordenamiento jurídico, mas no procederemos a avocarnos al desarrollo de dichas figuras al separarse de los lineamientos directivos de nuestra investigación.

De otro lado, en cuanto a aquellos comportamientos dispuestos por el Convenio de Budapest, pero ausentes de normativa nacional, puede hacerse referencia a los siguientes:

En primer lugar, en cuanto al artículo 7, cuyo asunto está vinculado al tema de la falsificación informática, el cual describe un requerimiento a los Estados a efectos de que introduzcan esta figura que se materializará cuando se produzca una introducción, alteración, borrado o supresión deliberados e ilegítimos de datos informáticos, la cual conlleve a la dación de datos informáticos carentes de autenticidad con propósitos legales, con independencia de que los

mismos posean una legibilidad o no. Lo resaltante de dicha modalidad es que, a los Estados si optaban por hacerlo, se les concedía la facultad de imponer una necesaria intencionalidad, un ánimo de perjuicio, en el desarrollo de la conducta punible. De su terminología expuesta es viable extraer dos conclusiones: Primero, es factible interpretar que el legislador no considero esta figura al entenderlo como un pleonasmo del tipo penal "atentado contra la integridad de los datos informáticos"; segundo, esa posición de calificar o no como doloso a este tipo penal podría haber ido en contra de la mentalidad legislativa peruana que, como puede verse, ha priorizado un accionar intencional (dolo), distanciándose del tema de la culpabilidad. A ello debemos señalar de que si bien sería superfluo ingresar a estos temas de repetir ciertas conductas en 2 o más normativas (sea civil, penal, laboral, constitucional u otras ramas jurídicas) lo cual podría generar confusión en el intérprete de la norma específica, lo cierto es que, a nuestro considerar, es que este tema de falsificación informática podría haber ingresado como una agravante del delito informático de atentado contra la unidad de datos informáticos, ya que nos encontramos a un contexto sumamente relevante, como lo es el caso de afectar datos informáticos con el propósito de dotarles de autenticidad insignificante para los propósitos, por ejemplo, probatorios, en el marco de un proceso judicial.

En segundo lugar, con referencia al artículo 16, se puede denotar un comportamiento que fortalecería el tipo penal que venimos aclamando (deber de conservar información por parte de la entidad, a través de indistintos actores, cuando la misma es imprescindible para fines de interés público) el cual encuadra de forma idónea los hechos acontecidos en el marco de la controversia, en investigación, que rodea al plan de gobierno digital de OSITRAN 2019-2022. Además, teniendo en cuenta que el marco jurídico argentino sí dispuso la concepción del referido tipo penal

reclamado, creemos que el punto de partida para dicho concepto a sancionar se origina en este artículo 16.

Dicho artículo enuncia que los Estados implementen las medidas conducentes a que sus autoridades respectivas, en el marco de las instituciones pública que representan, emitan los parámetros conducentes a salvaguardar los datos informáticos admitidos en un sistema informático, de los cuales exista el peligro y certeza inminente que pueda ser pasibles de alteración y/o sustracción. Pues bien, es de referir que este artículo actúa como una especie de actuación cautelar, preventiva, ante una eventual conducta que sustraiga los datos informáticos, indispensables de conservar, para fines de relevancia pública; por consiguiente, se puede reafirmar la particularidad de este artículo como fortalecedor de un tipo penal base que sancione la pérdida intencional de datos informáticos, por parte de un sujeto X, cuya preservación es necesaria para temas de seguridad nacional o de interés público.

En resumen, teniendo en cuenta los delitos informáticos aplicados y los no aplicados por la normativa peruana, se puede dar fe de una adecuada intención legislativa de sancionar conductas que propician la llamada ciber-delincuencia (producto de los delitos informáticos), aunque ello no lo exime al legislador peruano de encontrarse rodeado de cuestionamientos al no contemplar figuras que se consideran esenciales, como la agrupación de un tipo penal base que sancione la pérdida intencional de datos informáticos, por parte de un sujeto X, cuya preservación es necesaria para temas de seguridad nacional o de interés público, así como de su complemento preventivo explicado.

## Gobierno digital

### *Acepción de gobierno digital.*

Por un lado, se ha señalado que gobierno digital en su formato cuya concreción exitosa se apoya en las llamadas TIC, de forma tal que se genera una administración pública con atributos básicos de eficiencia, eficacia, transparente y de sencillo acceso para brindar servicios públicos a los diversos sectores que componen una comunidad (empresas, ciudadanos). Dichas TICS hacen pasible de manera fácil y rápida la reciprocidad de la información y servicios, de manera que se fortalece y aumenta el marco de vinculación entre ciudadanía, empresa y personal de la institución, para con la entidad que implementa el proyecto de gobierno digital. Es de señalar el alcance del gobierno digital comprende tanto componentes tecnológicos, como elementos culturales y de gestión de la información (Alfaro & Bustos & Gonzáles & Loroño, 2005).

En otra forma de pensamiento, se ha resaltado que el gobierno digital implica una vinculación con las famosas TIC, en razón de edificar una novedad en la forma de construir las relaciones internas y externas, del gobierno digital, para con el poblador, el gremio empresarial, los trabajadores públicos de la entidad que dispone el gobierno digital u otras ONG. (La Red, 2012).

En una tercera concepción, se ha referido que por gobierno electrónico, digital, e-government u otra variada clasificación terminológica que encuadre el vocablo referido, debe entenderse un agrupado de procesos y sistemas que sirvan de sustento a los primeros, de forma tal que se posibilite el acceso telemático tanto a nivel personal (por parte de los gestores de la entidad) como para con los destinatarios ajenos a la entidad (usuarios) respecto a los servicios puestos a disposición por la administración pública, sea para consultas en materia de una información digital específica como para la teletramitación (Riascos & Martínez & Solano, 2008).

### *Objetivos y fundamento de implementar el gobierno digital.*

Por un lado, cuando buscamos referirnos a los objetivos, propósitos, metas, finalidades de insertar un proyecto de gobierno digital, por parte de una entidad pública determinada, es de manifestar nuestra concordancia con lo esbozado por de la Red (2012), en razón de que dichos objetivos pueden sintetizarse así:

- Generar un sistema de gobierno cuya principal particularidad sea la transparencia en su funcionamiento a efectos de recuperar la confianza ciudadana y elevar, precisamente, la colaboración ciudadana producto de su participación.
- Desarrollar un gobierno con profesionalismo, en razón de disponer un agrupado de servidores y funcionarios públicos de calidad.
- Promover un marco de gobierno con la calidad como su principal sustento, a fin de delinear una expectativa de ser eficaces (de ser el caso, superar) en la meta de satisfacer la expectativa comunitaria, en cuanto a los servicios prestados, procurando una mejora, mayor accesibilidad y calidad en el objeto de la prestación
- Consolidar un gobierno digital que cuente como su principal razonamiento el fortalecimiento de las directrices relativas al acceso a la información y servicios públicos, de manera tal que dicho ciudadano que requiera el servicio concreto pueda tomar conocimiento de su requerimiento con independencia de su ubicación (casa, oficina, etc.). Es claro que esto propiciaría un nuevo modo de interrelacionarse con la sociedad y una modernidad en su funcionamiento de la entidad.
- Garantizar la existencia de un gobierno con mejora regulatoria, de manera tal que el ciudadano disponga de la certeza en torno a que su trámite sea realizará procurando la

eficacia, eficiencia y la calidad por la administración pública en su marco de gobierno digital.

De otro lado, se ha expresado que los objetivos del gobierno digital se concentran en la promoción del empleo y aprovechamiento de las connotadas TICS, de manera que pueda garantizarse progresivamente la presencia de un Estado y un ciudadano con cualidades de competitividad (la entidad, al contar un amplio grado de preparación en la inserción de sus políticas pertinentes; el ciudadano, al poseer una serie de capacidades y recursos idóneos-digitales que le posibiliten la interacción con el ente gubernamental), proactivo (la entidad, al adoptar un comportamiento que anticipe, prevenga aquellos riesgos o eventuales daños producto de un manejo incorrecto de las TICS, lo cual impone un seguimiento constante por sus agentes públicos; el ciudadano, al intervenir como un apoyo en el diseño del marco de trámites, políticas, proyectos, mediante la utilización de formas digitales), innovador (la entidad, al promover un intercambio y colaboración de ideas entre sus agentes públicos con la meta de la edificación del valor público; el ciudadano, al operar como un soporte que permita descubrir y solventar las principales disyuntivas y requerimientos comunitarios), así como su fin último sea la producción continua del llamado valor público, a partir de contextualizarnos en un ámbito de confianza digital. Esto último del valor público puede concebirse como la finalidad última de emplear los medios tecnológicos en el marco de comprender la relación gubernamental-poblacional. Verbigracia, se factoriza dicho valor público en el desarrollo social, la gobernanza, la garantía de derechos, la satisfacción de necesidades y la prestación de servicios de calidad, los cuales, de forma agrupada, coadyuvan a solucionar problemas verídicos. Mientras que el tema de la confianza digital se relaciona como una particularidad a observar en el campo donde se materializan las vinculaciones entre lo estatal, el

ciudadano y demás actores del ecosistema digital. Por ende, dicho campo debe corresponder a una sencillez, responsabilidad, previsibilidad y seguridad (MINTIC, s.f.)

En otro agrupado de vocablos, con relación a la motivación de materializar un gobierno digital/electrónic/ e-government, puede describirse los siguientes argumentos, en concordancia a De la Red (2012), de la siguiente manera:

- Facilita el manejo del internet y las conocidas redes de carácter telemático a efectos de operar como canales de comunicación entre la autoridad gubernamental y el ciudadano, a fin de complementar a los mecanismos de comunicación ya existentes (físicos).
- Denota para la ciudadanía la imagen de una administración estatal que se mantiene en constante actividad de laborar para prestar los servicios necesarios e indispensables para la ciudadanía, así como viabilizar la dación de inherencia de los administrados en sus decisiones.
- A partir de la construcción, consolidación y seguimiento de un proyecto de e-government, se faculta a la administración pública la potestad de optimizar sus disponibilidades humanas, técnicas y presupuestarias.
- El manejo con calidad, eficiencia y eficaz de las denominadas TICS coadyuvará a un empleo pertinente de la información administrativa y la relativa a la ciudadanía
- A partir de la relevancia reafirmada, una vez más, al internet, es que se autoriza a los sectores sociales y culturales el ingreso al entorno de vinculaciones entre los mismos para con el ente gubernamental en sus diversas manifestaciones, ya que anteriormente se encontraban privados de dicha permisibilidad.

### *Ciber-seguridad o seguridad electrónica*

Sobre este apartado, es de entender que a la llamada ciber-seguridad, seguridad electrónica o seguridad informática se la concibe como un marco que busca identificar y anticiparse ante cualquier manejo desautorizado de un sistema informático. Es decir, conlleva a desprender una estructura de protección frente a transgresores de los recursos informáticos, sea por buscar un provecho particular o por disponer un ánimo de malicia, causar un daño, producto de su accionar, aunque tampoco se descarta que dicho acceso pueda darse por accidente, por lo que de ser este último caso se estará en función al análisis de las particularidades concretas con el objetivo de determinar la existencia o no, de una eventual responsabilidad penal. Ahora bien, para elaborar sus fines protectores, de identificación y preventivos al accionar ilícito informático, se cuentan con programas o medios de defensa, entre otros, los antivirus, firewalls u otros medios símiles de resguardo frente a un atentado informático, ya sea por un agente de la institución como por un extraño a la misma (Universidad Internacional de Valencia, s.f).

Asimismo, se ha referido que las principales áreas que fundamentan a la seguridad informática son 1) la confidencialidad, en razón de que única y exclusivamente los agentes con el debido permiso y sin ánimo de generar perjuicio, son los que pueden ingresar a los indistintos recursos informáticos; 2) integridad, ya que única y exclusivamente el actor con los permisos requeridos y sin ánimo de ocasionar un menoscabo es quien debe ser capaz de modificar los recursos informáticos, de ameritarlo el caso; 3) disponibilidad, en razón de que la base de datos informáticos debe encontrarse presta al requerimiento del ciudadano, cuando sea necesario su debido conocimiento; 4) autenticación, a fin de acreditar la veracidad entre los sujetos que se comunican informáticamente, de forma que se evita el clásico delito de suplantación informática (Universidad Internacional de Valencia, s.f).

En otro parecer, se ha manifestado que, por ciberseguridad o seguridad digital debemos comprender la práctica reiterado de proteger los medios informáticos (computadoras, servidores, datos informáticos, etc) frente a aquellas conductas cuyo propósito es generar una afectación a dichos medios informáticos (Kaspersky, s.f).

Incluso, se ha llegado afirmar que por las conductas que contravendrían el ordenamiento y practicidad de la seguridad informática son 3: El ciber-crimen, la cual implica la presencia de actores individuales u organizados en estructuras cuya dirección a seguir en los ataques a los recursos informáticos es la generación de provechos financieros. La ciberguerra, a fin de recopilar datos informáticos con meros propósitos políticos de enfrentamientos entre actores gubernamentales de los diversos países. El ciber-terrorismo, siendo su única inspiración la de vulnerar los sistemas informáticos con la meta de propiciar pánico y/o temor, en la ciudadanía (Kaspersky, s.f).

Finalmente, también se considera como válida la alusión en cuanto a que la seguridad digital es un ámbito de la informática orientada a la protección de la infraestructura computacional y todos aquellos aspectos que puedan derivarse de la mencionada infraestructura. Por tanto, para lograr dicha finalidad, se ha dispuesto que el curso de acción se apoye en estándares, protocolos, métodos, reglas, herramientas y normas jurídicas destinadas a tratar de conducir a la exigüidad los hipotéticos riesgos a la infraestructura o información (Certsuperior, 2015).

### *Participación ciudadana digital y rendición de cuentas*

Como idea introductoria, hemos de referir que los diferentes Estados del mundo y sus agentes gubernamentales, en el proceso del siglo XXI, han ido desarrollando mayores mecanismos que coadyuven a una intervención más activa de la ciudadanía a efectos de que el resultado de

dicha participación se genere un colaboración en la manifestación de los respectivos mandatos constitucionales de cada país, de manera tal que se garantice la preservación del modelo democrático a regir, en teoría, en la mayor parte de los países a nivel global. (Riascos & Martínez & Solano, 2008)

Justamente, una de tales estrategias o formas innovadoras de promover la participación ciudadana responde a la utilización del internet y sus derivados en el marco de diversas vertientes, pero principalmente, en el proceso de impulsar la edificación, crecimiento y monitoreo al proceso de implementar el gobierno electrónico. De ahí, que si se llega a desarrollar la aspiración estatal no solo se promoverá lo que se nomina como participación digital ciudadana sino, además, se generaran un conglomerado de ventajas que puede resumirse como el acceso a la información, el conocimiento de la realidad país, la eficacia para el logro de los objetivos propuestos; la solidez y la evolución en los procesos y la eficiencia en el manejo de recursos estatales (Riascos & Martínez & Solano, 2008).

Ahora bien, prosiguiendo el concepto referido de participación digital ciudadana, tenemos de que si bien dicha vinculación entre el poblador y el sujeto gubernamental se construye en base a los componentes de un modelo arreglado a la democracia y al Estado de Derecho, como el caso de la Norma Suprema y sus complementarias leyes, dicha situación se enmienda con las ventajas que propicia el referido gobierno digital, de manera que se cumplan las funciones, se prestan los servicios de forma eficiente y se reducen excesivas formalidades que contravienen a los postulados del renombrado principio de celeridad en la actuación de la administración pública. Y todo ello se concreta sin dejar a un lado la vinculación entre gobierno y ciudadanía, por lo que transitamos de una acepción de participación ciudadana a una de participación digital ciudadana (Riascos & Martínez & Solano, 2008).

Finalmente, en torno al tema de garantizar un adecuado proceso de rendición de cuentas a partir del proceso progresivo de implementar un gobierno digital, se puede decir que el mismo se construye en base a la siguiente premisa: Si bien las administraciones centrales y regionales desarrollan un frecuente uso del internet para modernizar su marco de gestión y un esquema de gobernanza para fortalecer el contexto de relación entre ciudadano y Estado, lo cierto es que dicha rendición de cuentas o mejor dicho, el conocimiento de los resultados acontecidos, producto de la concreción de las acciones referidas, siempre se encontrará garantizado, no obstante, la alícuota o grado de avance en la construcción del gobierno digital y sus derivados se sujetarán a ciertos índices de educación dependiendo del país concreto y en menor medida, al asunto de las telecomunicaciones. Este modo de pensar fundamenta un elevado nivel de desarrollo que permitiría a los países superar las modalidades tradicionales de servicio y mejorar su eficacia y eficiencia. (Lara & Pina & Torres, 2013)

### *Marco normativo del Gobierno digital a nivel nacional*

Como bien se señaló, las directrices nacionales en materia de gobierno digital se regulan en función del citado Decreto Legislativo N°1412, del cual procederemos a resaltar sus particularidades más relevantes.

De conformidad a su artículo 6, el cual regula lo pertinente al concepto de gobierno digital, se puede señalar que el referido Decreto Legislativo N° 1412 (2018) concibe que el gobierno digital es:

> (…) Es el uso estratégico de las tecnologías digitales y datos en la Administración Pública para la creación de valor público. Se sustenta en un ecosistema compuesto por actores del sector público, ciudadanos y otros interesados, quienes apoyan en la implementación de

> iniciativas y acciones de diseño, creación de servicios digitales y contenidos. (…) Comprende el conjunto de principios, políticas, normas, procedimientos, técnicas e instrumentos utilizados (…) para la digitalización de procesos, datos, contenidos y servicios digitales de valor para los ciudadanos (Decreto Legislativo N° 1412, 2018).

Después, con relación al artículo 7 del aludido Decreto Legislativo N°1412 (2018), que concibe lo referente a los objetivos del gobierno digital:

> Normar las actividades de gobernanza, gestión e implementación en materia de tecnologías digitales (…); coordinar, integrar y promover la colaboración entre las entidades de la Administración Pública; promover la investigación y desarrollo en la implementación de tecnologías digitales (…); promover y orientar la formación y capacitación en materia de gobierno digital y tecnologías digitales en todos los niveles de gobierno (Decreto Legislativo N° 1412, 2018).

Posteriormente, en lo relativo a la identidad digital, de conformidad al artículo 10 del Decreto Legislativo N°1412 (2018), se la ha conceptuado como: "(…) Aquel conjunto de atributos que individualiza y permite identificar a una persona en entornos digitales".

Luego, en lo relativo a la llamada Infraestructura Nacional de Datos, en base al artículo 24 del Decreto Legislativo N° 1412 (2018), se le ha brindado la siguiente acepción:

> (…) Conjunto articulado de políticas, normas, medidas, procesos, tecnologías digitales, repositorios y bases de datos destinadas a promover la adecuada recopilación, procesamiento, publicación, almacenamiento y puesta a disposición de los datos que gestionan las entidades de la Administración Pública (Decreto Legislativo N° 1412, 2018).

Aparte, en lo que se refiere a la llamada interoperabilidad, la misma se la comprende, en concordancia al artículo 26 del Decreto Legislativo N°1412 (2018), como lo siguiente:

> (…) Es la capacidad de interactuar que tienen las organizaciones diversas y dispares para alcanzar objetivos que hayan acordado conjuntamente, recurriendo a la puesta en común de información y conocimientos, a través de los procesos y el intercambio de datos (…) (Decreto Legislativo N° 1412, 2018)

Por último, en lo que concierne a la seguridad digital la misma puede definirse, en compatibilidad al artículo 30 del Decreto Legislativo N°1412 (2018), en las siguientes palabras:

> La seguridad digital es el estado de confianza en el entorno digital que resulta de la gestión y aplicación de un conjunto de medidas proactivas y reactivas frente a los riesgos que afectan la seguridad de las personas, la prosperidad económica y social, la seguridad nacional y los objetivos nacionales en dicho entorno (…) (Decreto Legislativo N° 1412, 2018).

A partir de lo anterior, se debe señalar que la normativa nacional en materia de gobierno digital busca continuar la ruta de atención y ceñimiento a los lineamientos imprescindibles y formadores de todo plan, marco de gobierno digital. Prueba de ello, por un lado, se encuentra en haber recibido y estipulado la noción de gobierno digital, debiendo resaltarse de la definición propuesta por el legislador nacional el hecho de consolidar la mentalidad de que todo procedimiento, política, instrumento y/o herramienta, a través de las cuales se manejan las denominadas tecnologías de la información, se inspiran en la generación asidua y continua del connotado “valor público”. En adición, puede visualizarse que los objetivos del marco de gobierno digital nacional se alinean a la esencia de la finalidad de un gobierno digital, descrita en un párrafo

anterior, al aludir que todo gobierno digital busca apoyarse en las TICS para alcanzar el grado del mejor contexto de gobernanza y gestión de sus entidades, así como el hecho de permitir a los operadores públicos (funcionarios y servidores públicos) desarrollar sus actividades con la vista puesta en capacitarse en el uso de las TICS para transmitir la propuesta de valor (bienes y servicios), a la ciudadanía. Asimismo, respecto al tema de la identidad digital, es claro que la misma se ubica como un aspecto imperativo para conformar todo proyecto de gobierno digital, debido a que si cada sujeto que concurre en el marco de interacción estado-población no cuenta con un modelo idóneo de identificación, es factible que se susciten dilemas para dicho actor, ya sea que no pueda acceder a un determinado bien o servicio (ciudadano), cumplir las finalidades (agente público) u otras circunstancias indeseables que puedan mencionarse. Por último, es claro que otros 2 pilares de todo gobierno digital son la llamada interrelación entre los agentes públicos e instituciones que participan en la ejecución del proyecto de gobierno digital, pero, a su vez, dicha vinculación debe materializarse en un ambiente de confianza, equivalencia y estabilidad, lo cual, precisamente, debe encontrarse certificado por un contexto donde se imponga la seguridad digital frente a cualquier tipo de amenaza digital.

### *Regulación del gobierno digital en el contexto comparado*

Con relación al marco comparado o extranjero, en materia de proyectos, planes de gobierno digital, queremos hacer alusión a 3 sistemas específicos: Colombia, México y España.

En primer lugar, abordando el marco normativo colombiano en el asunto del gobierno digital, la regulación jurídica a la que debemos remitirnos es la vinculada al Decreto N°1008 (2018), del cual corresponde abordar sus especificidades más pertinentes.

Por un lado, en lo relativo a los principios que orientan el desarrollo del gobierno digital, de conformidad a su artículo 2.2.9.1.1.3 del Decreto N°1008 (2018), encontramos los siguientes:

> (…) Innovación: (…) El Estado y los ciudadanos deben propender por la generación de valor público a través de la introducción de soluciones novedosas que hagan uso de TIC, para resolver problemáticas o necesidades identificadas. Competitividad: (…) Los ciudadanos deben contar con capacidades y cualidades idóneas para actuar de manera ágil y coordinada, optimizar la gestión pública y permitir la comunicación permanente a través del uso y aprovechamiento de las TIC. Proactividad: (…) Se busca que el Estado y los ciudadanos trabajen de manera conjunta en el diseño de políticas, normas, proyectos y servicios, para tomar decisiones informadas que se anticipen a los acontecimientos, mitiguen riesgos y atiendan a las necesidades específicas de los usuarios (…). Seguridad de la Información: (…) Busca crear condiciones de uso confiable en el entorno digital, mediante un enfoque basado en la gestión de riesgos preservando la confidencialidad, integridad y disponibilidad de la información de las entidades del Estado, y de los servicios que prestan al ciudadano (Decreto N°1008, 2018).

Después, en lo que concierne a los componentes y propósitos de la estructura del gobierno digital colombiano, de conformidad a su Decreto N°1008 (2018) y a su artículo 2.2.9.1.2.1, se menciona a los siguientes:

> (…) 1.1. TIC para el Estado: Tiene como objetivo mejorar el funcionamiento de las entidades públicas y su relación con otras entidades públicas (…) 1.2. TIC para la Sociedad: Tiene como objetivo fortalecer la sociedad y su relación con el Estado en un entorno confiable que permita la apertura y el aprovechamiento de los datos públicos, la

> colaboración en el desarrollo de productos y servicios de valor público, el diseño conjunto de servicios, la participación ciudadana en el diseño de políticas y normas, y la identificación de soluciones a problemáticas de interés común. 2. Habilitadores Transversales de la Política de Gobierno Digital (…) 3. Lineamientos y estándares de la Política de Gobierno Digital (…). 4. Propósitos de la Política de Gobierno Digital: (…) 4.1. Habilitar y mejorar la provisión de servicios digitales de confianza y calidad. 4.2. Lograr procesos internos, seguros y eficientes a través del fortalecimiento de las capacidades de gestión de tecnologías de información. 4.3. Tomar decisiones basadas en datos a partir del aumento el uso y aprovechamiento de la información. 4.4. Empoderar a los ciudadanos a través de la consolidación de un Estado Abierto (…) (Decreto N°1008, 2018).

Finalmente, su artículo 2.2.9.1.4.1 se hace mención a una figura de seguimiento y evaluación la cual, concorde al Decreto N°1008 (2018), estipula lo siguiente:

> (…) El Ministerio de Tecnologías de la Información y las Comunicaciones, a través de la Dirección de Gobierno Digital, adelantará el seguimiento y evaluación de la Política de Gobierno Digital por medio de indicadores de cumplimiento e indicadores de resultado, de acuerdo con los criterios de evaluación y seguimiento definidos por el Consejo para la Gestión y Desempeño institucional (…) (Decreto N°1008, 2018).

En segundo orden de términos, en lo que se refiere al marco mexicano en la temática de gobierno digital, electrónico, tenemos que su respectiva Ley de Gobierno Electrónico (2015) abarca una serie de disposiciones normativas que resulta interesante de poner en conocimiento.

Por un lado, tenemos que el artículo 21 de Ley de Gobierno Electrónico de México (2015), contempla que la vinculación electrónica entre población y ente gubernamental puede materializarse en los siguientes términos:

> (…) Por vía electrónica todo tipo de solicitudes, escritos, recursos, reclamaciones y quejas. (…) Acceder por medios electrónicos a la información de los Órganos de la Administración Pública (…) Conocer la información relativa a los trámites y servicios de los Órganos de la Administración Pública, a través del sitio del Registro Electrónico de los Trámites y Servicios (Ley de Gobierno Electrónico de México, 2015).

Después, en lo que refiere al objetivo de propiciar un uso progresivo de los medios electrónicos a efectos de generar un clima de estabilidad digital, el artículo 34 de la Ley de Gobierno Electrónico de México (2015), manifiesta que: “La Administración Pública fomentará el acceso y uso de las tecnologías de la información y comunicaciones en los ciudadanos, para el desarrollo de una cultura digital ciudadana y de Gobierno Electrónico”.

Aunado a ello, en lo que se refiere al carácter de la información que se almacena en los sistemas informáticos de la entidad específica y el deber correspondiente sobre la misma, el artículo 39 Ley de Gobierno Electrónico de México (2015) plasma que:

> La información que generen, reciban o administren los Órganos de la Administración Pública y que se encuentre contenida en cualquier medio o soporte electrónico, informático o de cualquier otro derivado de innovaciones tecnológicas, se denominará genéricamente documento electrónico. Los documentos electrónicos deberán ser organizados, conservados y custodiados de acuerdo a lo establecido en la ley de la materia (Ley de Gobierno Electrónico de México, 2015).

En un tercer apartado de vocablos, tenemos al marco jurídico español el cual, conforme a su Ley N°39-2015, regula una serie de particularidades pertinentes en cuanto a la relación entre los administrados y el actor gubernamental, mediante las renombradas tecnologías de la información y de la comunicación. Ahora bien, el hecho de que dichas disposiciones no hayan sido encajadas en una normativa que se dedique solamente al tratamiento del gobierno electrónico (fueron encajadas en una ley que define los principales aspectos del procedimiento administrativo común de las administraciones públicas), como en el caso colombiano y mexicano, no le disminuye la relevancia que ameritan aquellas reglas que dispongan la vinculación entre administración pública y ciudadanía, lo cual constituye la esencia de un buen plan de gobierno digital en todo sistema público.

En un acápite, se concibe que los ciudadanos disponen de algo que llamaremos "derechos de interrelación electrónica", para con la administración pública, conforme puede verse de la Ley 39-2015 en su artículo 13, en el siguiente vocabulario:

> **(…)** A comunicarse con las Administraciones Públicas a través de un Punto de Acceso General electrónico de la Administración; (…) a ser asistidos en el uso de medios electrónicos en sus relaciones con las Administraciones Públicas; (…) a utilizar las lenguas oficiales en el territorio de su Comunidad Autónoma, de acuerdo con lo previsto en esta Ley y en el resto del ordenamiento jurídico; (…) al acceso a la información pública, archivos y registros (…) (Ley N°39, 2015).

Asimismo, puede observarse que el artículo 14 de la referida Ley 39-2015 fortalece nuestra posición de construir un "derecho de interrelacionarse electrónicamente", ya que dicho precepto

contempla a los sujetos obligados a concretar la vinculación electrónica con la administración pública, al señalar lo siguiente:

> **(…)**
>
> 2. En todo caso, estarán obligados a relacionarse a través de medios electrónicos con las Administraciones Públicas para la realización de cualquier trámite de un procedimiento administrativo (…)
>
> a) Las personas jurídicas.
>
> b) Las entidades sin personalidad jurídica.
>
> c) Quienes ejerzan una actividad profesional para la que se requiera colegiación obligatoria, para los trámites y actuaciones que realicen con las Administraciones Públicas en ejercicio de dicha actividad profesional (…)
>
> d) Quienes representen a un interesado que esté obligado a relacionarse electrónicamente con la Administración.
>
> e) Los empleados de las Administraciones Públicas para los trámites y actuaciones que realicen con ellas por razón de su condición de empleado público (…) (Ley N°39, 2015).

En función de todo lo visto en este capítulo, se puede desglosar los términos más relevantes por cada marco de gobierno digital. En el campo colombiano, debe hacerse mención de la importancia de unificar todos sus principios, como la competitividad, innovación o seguridad de la información, los cuales se enmarcan como los parámetros que deben tener en cuenta no solo los agentes públicos, sino también la sociedad al momento de efectuar su facultad de vincularse electrónicamente con la sociedad.; esto último puede comprobarse al haberse

descrito, en un apartado de la normativa colombiana, que las TICS (mecanismo sustancial del gobierno digital) posee su campo de aplicabilidad, de una u otra forma, para el Estado como para la sociedad; asimismo, es de rescatar esa obligación de monitoreo y seguimiento, respecto a la ejecución de todo plan de gobierno digital, por parte de las entidades públicas colombianas, a fin de evitar desperfectos o contravenciones a la normativa de dicho país, conforme puede entenderse del razonamiento legislativo de tal sistema jurídico. En lo que se refiere al ordenamiento mexicano, debe destacarse la prioridad de su legislador de sentar, taxativamente, la necesidad de que la ciudadanía se relacione con la autoridad gubernamental, de forma electrónica, mediante la utilización de abundantes vías. Por si fuera poco, más que una facultad atribuida a la ciudadanía, se lo considera como una imposición a los sectores de la administración de forma tal que se amplié y conserve el ideal de gobierno electrónico y de cultura digital. Pero sobretodo, lo que más debe resaltarse de las reglas jurídicas mexicanas en materia de gobierno electrónico, al igual que en el caso argentino cuando se abordó lo relativo a delitos informáticos, es el tema de garantizar a la ciudadanía la existencia de un deber de preservación de toda aquella información, dato y/o hecho abarcado en los sistemas informáticos de sus respectivas agencias que componen la integridad llamada administración pública. En lo que corresponde al marco español, lo que debe aplaudirse del emisor español de la normativa en asuntos electrónicos está referido a su disposición en torno de que las vinculaciones de la ciudadanía y autoridad gubernamental, más que constituir una obligación de ser fomentada y promovida por este último, se constituyen, literalmente, como un derecho de los administrados. Pero no por ello se exime a la población española de atender a que la misma también debe ser recíproca en el trato electrónico, ya que se determina que agentes de la sociedad civil tiene un deber de efectuar sus vinculaciones con lo gubernamental, por los mecanismos digitales.

### *Gobierno digital en el supuesto supranacional*

En cuanto al marco supranacional, hemos de señalar que el principal instrumento internacional que abarca en su seno la temática de gobierno digital es la llamada Carta Iberoamericana de Gobierno Electrónico (2007). Al igual que en el caso del Convenio sobre la Ciberdelincuencia, esta herramienta internacional ha servido de orientación para los Estados a efectos de diseñar e implementar las medidas necesarias para hacer efectivo su proyecto de gobierno electrónico, en sus diferentes dependencias, entidades que componen sus respectivas administraciones públicas. Por consiguiente, procederemos a destacar los acápites más relevantes de este documento, para los fines de nuestros propósitos investigativos.

Por un lado, en cuanto a la importancia de acoger un modelo de gobierno electrónico por la administración pública, la Carta Iberoamericana de Gobierno Electrónico (2007), en sus artículos 4 y 5 propugna que:

> (…) Se propone la satisfacción de las necesidades así como contribuir al desarrollo de la sociedad, por lo que jamás podrá consistir en una simple respuesta a las ofertas tecnológicas que provienen del mercado (…) En atención a que (…) se encuentra indisolublemente vinculado a la consolidación de la gobernabilidad democrática, tiene que estar orientado a facilitar y mejorar la participación de los ciudadanos en el debate público y en la formulación de la política en general o de las políticas públicas sectoriales (…) (Carta Iberoamericana de Gobierno Electrónico, 2007).

Después, es de visualizar que la propuesta de un “derecho a interrelacionarse electrónicamente”, concedido al ciudadano para con la administración, ha sido tolerado por la Carta Iberoamericana de Gobierno Electrónico (2007), al referir su artículo 7 que:

> La implantación del Gobierno Electrónico comporta el reconocimiento por parte de los Estados Iberoamericanos del derecho de los ciudadanos a relacionarse electrónicamente con sus Gobiernos y Administraciones Públicas. Lo que supone que las Administraciones estén interrelacionadas entre sí a fin de simplificar los procedimientos (…) (Carta Iberoamericana de Gobierno Electrónico, 2007).

Aparte de lo anterior, se vuelve a enfatizar en la noción base del tema de la seguridad digital de todo gobierno electrónico, por lo cual la Carta Iberoamericana de Gobierno Electrónico (2007), en su artículo 13, expone que:

> (…) Los Estados iberoamericanos aprobarán, las normas jurídicas y técnicas y los actos ejecutivos necesarios para que los ciudadanos y las Administraciones Públicas en sus relaciones electrónicas puedan tener seguridad y confianza, tanto en lo que se refiere a la identidad de la persona, órgano o institución que se comunica, como en lo que se refiere a la autenticidad e integridad del contenido de la comunicación, así como, consecuentemente, en la imposibilidad de ser repudiada por el emisor (Carta Iberoamericana de Gobierno Electrónico, 2007)

En otro lado, respecto a las medidas necesarias que guían el régimen de los documentos y archivos electrónicos, tenemos que la Carta Iberoamericana de Gobierno Electrónico (2007), en su artículo 16, dispone que:

> Los Estados regularán los documentos y archivos electrónicos sobre la base de (…) a. Equivalencia de los documentos electrónicos con los documentos en papel. Ello implica que los particulares o las Administraciones Públicas pueden aportar a los expedientes, o utilizar en sus relaciones con otras Administraciones Públicas o con terceros,

> documentos electrónicos (…) b. Validez: Los documentos tramitados electrónicamente por los ciudadanos mantienen la misma validez intrínseca de aquellos que puedan serlo físicamente, (…). c. Conservación y gestión de los datos. Los documentos, actos y actuaciones electrónicas deberán guardase en archivos electrónicos que garanticen la integridad, autenticidad, mantenimiento y conservación sin posibilidades de manipulación o alteración indebida. Las Administraciones Públicas asegurarán que tales documentos sean accesibles (…) La Administración Publica gestionará las bases de datos garantizando la calidad de la información contenida y establecerá los mecanismos necesarios para la prevención y recuperación (…) de forma tal que se reduzca al mínimo la posibilidad de riesgo de pérdida de datos y se asegure la efectiva recuperación de los mismos en caso de contingencia (…) (Carta Iberoamericana de Gobierno Electrónico, 2007).

Si bien es cierto que la normativa internacional en visualización desglosa disposiciones ya comentadas en el apartado nacional y comparado, se hace indispensable el comentario respectivo debido a que la misma constituye el cimiento sobre el cual se construyeron los planes de gobierno digital internos, de cada legislación. Siendo así, se hace importante enfatizar que la propuesta de gobierno digital no se circunscribe a un mero ofrecimiento de la administración pública hacia el ciudadano, sino que se constituye en un derecho y deber, por parte de ambos sujetos, de entender al modelo de gobierno digital como una novedad de poder observar ejecutadas sus relaciones, mediante herramientas sencillas, céleres y simplificadoras de trámites innecesarios. Además, una disposición que parece haber sido acatada por todos los Estados es el tema de la seguridad digital, ya que en todas las regulaciones jurídicas estudiadas hasta el momento ninguna de ellas ha hecho caso omiso a lo imprescindible de ser aplicada en la

sociedad de que se trate. Finalmente, un acápite adicional a tener en cuenta es que esta Carta Iberoamericana hace mención a la imperiosidad de que los gobiernos adopten las medidas legislativas pertinentes cuyo objetivo sea la preservación de aquella información digital agrupada en los sistemas digitales de la entidad, así como certificar los procedimientos de recuperación, ante un eventual caso de pérdida. Ante ello, volvemos a hacer un llamado de atención respecto a que si bien el Estado peruano concuerda en esta disposición con la Carta (ello se comprueba por disposiciones del DL 1412 que estipulan la existencia de un registro de datos, infraestructura nacional de datos, entre otras directrices) al señalar el deber de fiscalizar conductas que pudieran atentar contra dicho mandato, no se observa dicho equilibrio conductual en referencia a describir un tipo penal en el ordenamiento jurídico peruano que sancione, textualmente, el ámbito de transgredir la obligación de conservar la información y proscribir toda conducta que tienda a la pérdida o sustracción de la misma, lo cual conduce a complejidades al querer condenar el comportamiento punible (en todo caso, el tipo penal nacional que puede servir para sancionar el hecho punible es el atentado contra la integridad de datos/sistemas informáticos).

### *Aspectos relevantes del plan de gobierno digital 2019-2022 de OSITRAN*

En lo que concierne a las particularidades más relevantes del plan de gobierno digital 2019-2022 de OSITRAN (2019), pueden destacarse las siguientes:

> El Plan de Gobierno Digital del OSITRAN 2019-2022, tendrá como marco al Plan Estratégico Institucional del mismo periodo, documento que responde a la Visión del Sector y se encuentra a su vez alineado al Plan Estratégico Sectorial Multianual PESEM 2016-2020 (…) (Plan de gobierno digital 2019-2022 de OSITRAN, 2019, p.4).

Para ello, se debe tener en cuenta que la visión del sector, en articulación con el plan estratégico aludido, importa lo siguiente:

> (…) "*Mejorar la implementación de la gestión pública para resultados en todas las entidades públicas*", Acción estratégica 3.5 "*Promover el Gobierno electrónico como soporte a los procesos de planificación y gestión de las entidades públicas*", la misma que promueve la mejora de la eficiencia y eficacia de las entidades de la administración pública, a través del uso intensivo de las tecnologías de la información. (OSITRAN, 2019, p.4)

Después, en lo que se refiere a su objetivo de plan de desarrollo de la sociedad de la información en el país (o también llamada "agenda digital peruana 2.0"), se ha referido que:

> (…) Constituye una importante contribución de políticas para el cumplimiento de los Objetivos de Desarrollo del Milenio para el Perú, que identifica a las Tecnologías de la Información y la Comunicación (TIC), no como un fin en sí mismas, sino como un instrumento en la búsqueda de un desarrollo humano más equitativo y sostenible que haga posible un mayor crecimiento económico, el logro de mejores empleos y un aumento de la competitividad, inductora de la inclusión social (OSITRAN, 2019, p.5).

Teniendo en cuenta ello, es que la institución ha desarrollado lo que se denomina visión tecnológica de la entidad, la cual consiste y se declara en los siguientes vocablos:

> (…) Consiste en abordar y formular directrices que faciliten a la JTI la identificación de iniciativas tecnológicas orientadas, principalmente, a hacer viable la misión institucional del OSITRAN. (…) Se declara de esta manera: "*OSITRAN Digital. Al 2022 el OSITRAN es una entidad digital que entrega servicios eficientes a los usuarios y ciudadanos utilizando las tecnologías de la información, como resultado de su proceso de*

> *transformación digital, con seguridad, transparencia y predictibilidad."* (OSITRAN, 2019, pp.6-7).

Ahora bien, teniendo en cuenta las dificultades que presenta el llevar a cabo sus finalidades institucionales y la necesidad de adecuarse al marco tecnológico incesante, en el hoy en día, la institución señaló que:

> El OSITRAN en la etapa institucional en la que se encuentra, tiene planificado implementar soluciones de uso intensivo del Internet y de tecnologías digitales, como mecanismos para dar soporte adecuado a los procesos misionales y de gestión administrativa y estratégica. Para dicho fin, ha tenido a bien formular el presente Plan de Gobierno Digital, como instrumento orientador de las acciones de tecnologías de la información a implementar, a fin de garantizar su alineamiento a los objetivos institucionales y la contribución al logro de los mismos (OSITRAN, 2019, p.8).

Pero abordando lo más interesante, es de referir que, a partir de un estudio previo realizado por diversas de sus coordinaciones, a fin de identificarlas principales brechas digitales de la institución y que requieren resolverse a partir de la inserción progresiva del plan de gobierno digital de la entidad, se le concederá la prioridad a la mención de aquellas identificadas por la coordinación de aplicación, siendo dichas brechas, entre otras, las siguientes:

> (…) No se cuenta con un procedimiento documentado para el levantamiento de la demanda de requerimientos de los usuarios, para contar con nuevas aplicaciones o realizar cambios importantes a los sistemas actuales en producción, identificando las necesidades de automatización en los procesos misionales. (…) Las aplicaciones de entidad cuentan con mecanismos de seguridad básicos tales como control de acceso y auditabilidad, mas no se

han implementado controles adicionales de seguridad que permitan garantizar que el sistema no es vulnerable a amenazas informáticas. Es de mencionar que como parte de la NTP ISO/IEC 27001:2014, en la cláusula A.14 Adquisición, desarrollo y mantenimiento de sistemas, se establece el objetivo de Garantizar que la seguridad de la información es una parte integral de los sistemas de información a través del ciclo de vida completo (OSITRAN, 2019, pp.12-13).

***Particularidades del caso base de la investigación: Presunta supresión de información de relevancia pública de la base de datos de OSITRAN.***

El suceso que ha envuelto a OSITRAN en una controversia, como garante de información pública de la materia en su calidad de Organismo Supervisor de la Infraestructura y Transporte Nacional, responde a una supuesta supresión de correos y otra clase de documentación que respondía a 4 ex-funcionarios de dicha entidad. La información en discusión corresponde a 2017 y estaba vinculada en el marco de la firma de la adenda en el investigado caso “Chinchero”. En dichos correos, se manifestaba, por el remitente a los 4 ex-funcionarios, que se favorecía el otorgamiento de pagos mensuales a la concesionaria “Kunturwasi”, aunque luego se cambió de dicho parecer, pero la polémica se ubica en que todo el detalle referente a tales correos se suprimió de la base de datos de OSITRAN. Al respecto de ello, se debe tener en cuenta que el informe N°315-2017-JTI-GA-OSITRAN, estipulaba que cuando una persona cese en sus funciones no deberá eliminar sus correos electrónicos u otra documentación abarcada en sus computadoras, ya que la misma pertenece a la institución (OSITRAN). No obstante, ello, mediante el mismo informe se dio a conocer que los ex-funcionarios Patricia Benavente, Obed Chuquihuayta, Jean Paul Calle y Luis Robas eran aquellos a quienes pertenecían las computadoras donde se eliminó la información de interés público. Aunado a ello, mediante el informe de aquel entonces (2017) se

destacaba que no se contaba con un procedimiento de back ups (resguardo) ante estos casos de pérdida de información relevante (por lo que es claro que con la dación del DL 1412 y el plan de gobierno digital de OSITRAN 2019-2022, se hizo imperativo que dicho procedimiento de back up debía ser incorporado). La ausencia de la información, producto de la negligencia en disponer de backups, fue confirmado por el informe N°319-2017-JTI-GA-OSITRAN. A raíz de ello, si bien la Srta. Benavente deslindó que el borrado de información de su medio tecnológico fuera de su autoría, existen un sustento físico (se dejó constancia en el referido informe) de que el Sr. Chuquihuayta actúara como un autor mediato en dicho delito, al ordenar a un tercero la comisión de la infracción de borrar la información de relevancia pública. (Latina, 2019). Sin perjuicio de ello, si bien la propia institución, OSITRAN, a raíz del reportaje emitido, divulgó un comunicado mediante el cual se desmienten las aseveraciones expuestas por dicho programa, al señalar que la información perteneciente a los correos de los ex-funcionarios se encuentra perenne en sus sistemas de seguridad, lo cierto es que no es menester abordar en nuestro producto científico, como se ha podido observar, si hay responsabilidad o no en este caso. Claro que no. Dicha labor corresponderá ser dirimida por las autoridades correspondientes. Lo que buscamos, a partir de la proposición de este caso, es determinar, producto de lo acontecido en dicho caso, si ante esta presunta incursión en delitos informáticos (la acción antijurídica de este delito, reiteramos, no dispone de un tipo específico, el cual sancione la omisión del deber de conservar información que por su contenido sea de relevancia-interés pública, por lo cual podemos encontrarnos ante un acceso ilícito, un atentado contra la integridad de los datos/sistema informáticos, ante un fraude informático o ante una suplantación de identidad, según la perspectiva o modo de ver por el analista legal), en el progreso de que OSITRAN viene adoptando su plan de gobierno digital, puedan esperarse nuevas comisiones de delitos informáticos, las cuales contravendrían toda política abarcada en su proyecto de gobierno digital, como el caso de su Norma Técnica ISO 27001 de Seguridad de la Información.

## Definición de Términos Básicos

**Bien jurídico tutelado. -** Objeto de resguardo por las normas penales al ser de relevancia e interés público.

**Confianza digital. -** Particularidad impregnada en el marco del gobierno digital a través de la cual se observa un sentir bilateral entre la población y el agente del Estado que denota un clima de estabilidad en sus relaciones.

**Delitos informáticos. -** Comportamientos sancionados por las normas penales u otras de símil naturaleza, a través de la cual se incurren en conductas que contravienen el ambiente de equilibrio y paz en la sociedad, al emplearse mecanismos de la tecnología de la información y de la comunicación.

**Ecosistema digital. -** Ámbito en el cual se desarrollan de manera recíproca, eficiente y en igualdad de condiciones las vinculaciones entre la administración pública y la autoridad gubernamental, a través del empleo de herramientas digitales.

**Globalización digital. -** Fenómeno que describe un avance en las actitudes, comportamientos y medios que rodean a la sociedad, en este caso, implican una dirección hacia todo aquel objeto vinculado a la tecnología digital.

**Gobierno digital. -** Agrupado de principios, procedimientos, directrices y/o reglas mediante la cual se estructura un sistema de organización de la administración pública para vincularse con la población, agentes empresariales y actores al interior de la entidad respectiva.

**Identidad digital. -** Herramienta que permite dotar de un signo distintivo a cada agente o entidad pública que participa en las actividades que se desglosan de todo proyecto de gobierno digital.

**Participación ciudadana digital. -** Enfoque que asevera la esencialidad de observar una concurrencia activa de la sociedad en el marco de implementarse un proyecto de gobierno digital, tanto para recibir bienes y servicios u otra clase de prestación como para prestar colaboración, en lo necesario, a las actividades de lo gubernamental en asuntos digitales.

**Plan de gobierno digital. -** Bosquejo que contiene todas las reglas, parámetros y directrices que guiarán la inserción del sistema de vinculación digital Estado-sociedad, a través del gobierno digital.

**Seguridad digital. -** Garantía de que todas las actuaciones a desarrollarse en el ecosistema digital, producto de los parámetros derivados del gobierno digital, podrán aplicarse sin estar sujeto a algún tipo de contingencia al estar insertos mecanismos que prevengan afectaciones al marco digital y, en caso de haberlas, se pueda disponer lo necesario para recuperar los datos y solucionar las problemáticas que pudieran afectar al marco digital.

**Sociedad informática. -** Estructura novedosa mediante la cual la comunidad y sus diversos concurrentes se acomodan a los criterios que rigen el gobierno digital, electrónico o informático.

**Sujeto activo. -** Actor o entidad que desarrolla el ilícito sanciona por las normas penales, sea que actúe con dolo (intencionalidad) o culpa (omisión).

**Sujeto pasivo. -** Agente o entidad que soporta los efectos perniciosos de la concreción del comportamiento ilícito, perpetrado por el sujeto activo.

**Tecnologías de la información y comunicación. -** Conjunto de estrategias y técnicas mediante la cual se planifica y se ejecutan los postulados de gobierno digital a insertar en una administración pública-sociedad específica.

# Capítulo III: Marco Metodológico

## Enfoque de la Investigación

Se ha determinado que el enfoque de la presente investigación será de carácter mixto. Si bien es cierto que el presente producto científico se asocia más al ámbito de lo cualitativo, ya que nos basamos en aspectos dinámicos, por lo cual nos focalizamos en la experiencia subjetiva de los fenómenos, así como identificar, explorar y comprende dicho fenómeno, lo cierto es que la visión cuantitativa se presenta en razón de ser necesario un cierto muestreo de datos numéricos (encuesta), a fin de confirmar o refutar la hipótesis de nuestro trabajo, relativa a que los delitos informáticos inciden negativamente en la implementación progresiva del plan de gobierno digital de OSITRAN 2019-2022.

## Variables

## Operacionalización de variables

### *Variable independiente (X-1): Delitos informáticos.*

**Dimensiones:**

1. Respuesta a los delitos informáticos durante sus inicios.

2. Respuesta a los delitos informáticos en la actualidad.

**Indicadores:**

1. Acción antijurídica en el entorno digital.

2. Amenaza a la seguridad digital

3. Producto de la globalización digital de la sociedad.

***Variable dependiente (Y-2): Gobierno digital.***

**Dimensiones:**

1. Claves de éxito del gobierno digital por el comportamiento de la administración pública.

2. Claves de éxito del gobierno digital por la colaboración ciudadana.

**Indicadores:**

1. Uso de tecnologías de la información y comunicación.

2. Creación de valor público.

3. Ecosistema digital de gobierno

## Hipótesis

### Hipótesis General

- Los delitos informáticos inciden negativamente en la implementación progresiva del plan de gobierno digital de OSITRAN 2019-2022.

### Hipótesis Específicas

- Los delitos contra los datos y sistemas informáticos influyen negativamente en la implementación progresiva del plan de gobierno digital de OSITRAN 2019-2022.
- Los delitos informáticos contra el patrimonio afectan adversamente la implementación progresiva del plan de gobierno digital de OSITRAN 2019-2022.

- Los delitos informáticos contra la fe pública repercuten nefastamente en la implementación progresiva del plan de gobierno digital de OSITRAN 2019-2022.

**Tipo de Investigación**

Es de señalar que la presente investigación es de carácter correlacional, descriptivo y exploratorio.

Es de carácter correlacional, en razón de que se desarrolla un marco de interacción entre las variables del estudio (delitos informáticos y gobierno digital) para llegar a la obtención de un resultado específico; asimismo, se tiene presente que si una de ella se altera, dicho cambio incidirá en la otra. Ejemplo, si los delitos informáticos reducen su margen de concreción es claro que los propósitos del gobierno digital se verán fortalecidos (aumentará su grado de credibilidad).

Es de carácter descriptivo, en función de que el entendimiento de los fenómenos que se requieren interconectar (delitos informáticos y gobierno digital) imponen el dar a conocer sus principales características, particularidades.

Es de carácter exploratorio, debido a que los resultados de la investigación coadyuvarán al desarrollo de posteriores investigaciones. Es decir, si se demuestra que a partir del suceso controvertido acontecido en OSITRAN, los delitos informáticos son propensos a influenciar el marco de implementación de un plan de gobierno digital, se podrían desarrollar investigaciones futuras que cuestionen la pertinencia de proseguir la actual inserción del conglomerado de planes de gobierno digital de las indistintas entidades de la administración pública (MINSA, OSITRAN, OEFA, etc.)

## Diseño de la investigación

El diseño de la presente investigación se ajusta a un procedimiento de carácter experimental, así como se vale del empleo de un método inductivo.

Se sigue un modelo experimental, en razón de que se busca controlar una realidad, respecto a la influencia de los delitos informáticos en el proyecto de gobierno digital de OSITRAN, para lo cual se introduce, en el proceso de demostrar dicha incidencia, la descripción de un suceso que ha envuelto en un cuestionamiento a dicha institución, como lo es un presunto reportaje que ha dado a conocer una presunta supresión de información de interés público.

Nos basamos en un método inductivo, ya que se parte de lo específico a lo general en nuestra investigación; verbigracia, si se demuestra que los delitos informáticos son propensos a desarrollarse en los sistemas informáticos de OSITRAN, a pesar de que dicha entidad viene implementando un proyecto de gobierno digital, ello conllevaría a determinar que los delitos informáticos son factibles de acontecer en todas las entidades públicas de la administración pública peruana, a pesar de que algunas vienen ingresando un proyecto de gobierno digital.

## Población y Muestra

### Población

Se tiene como mentalidad realizar que el foco de atención (población) de la encuesta a realizar se constituya por estudiosos de los asuntos que atañen a las problemáticas, aspectos, del marco jurídico.

**Muestra**

Se ha delineado como muestra un total de 30 operadores del derecho a efectos de ser encuestados: 15 profesionales en ejercicio (abogados, fiscales, jueces, etc.) y 15 iniciantes en la materia jurídica, pero con sólidos conocimientos en la misma (estudiantes y egresados de la carrera de Derecho de la Universidad Peruana de Las Américas).

**Técnicas e Instrumentos de Recolección de Datos.**

Se empleará la encuesta como instrumento de recolección de datos, a fin de recoger las opiniones y pensamientos de voces autorizadas en materia jurídica, respecto a la hipotética incidencia de los delitos informáticos en la inserción progresiva del plan de gobierno digital 2019-2022 de OSITRAN, teniendo en cuenta el presunto suceso de supresión de información, cuya peculiaridad es la relevancia pública, de la base de datos de dicha institución pública. Asimismo, es de señalar que toda la información estadística será medida con el programa SPSS, el cual permitirá la evaluación completa para análisis de datos y creación de tablas gráficas a fin de responder cada una de las preguntas del instrumento utilizado para la encuesta, la cual realiza preguntas sobre cada una de las variables y dimensiones y correlacionarla con la variable dependiente.

# Capítulo IV: Resultados

## Análisis e interpretación de Resultados

### Comprobación de la hipótesis principal.

Los delitos informáticos inciden negativamente en la implementación progresiva del plan de gobierno digital de OSITRAN 2019-2022

***Tabla 1***

**¿Considera que es factible que se concreten acciones antijurídicas en torno a los datos y sistemas informáticos en OSITRAN, teniendo en cuenta su implementación progresiva de plan de gobierno digital 2019-2022?**

| | | Frecuencia | Porcentaje | Porcentaje válido | Porcentaje acumulado |
|---|---|---|---|---|---|
| Válidos | En desacuerdo | 5 | 16,7 | 16,7 | 16,7 |
| | Ni de acuerdo ni en desacuerdo | 12 | 40,0 | 40,0 | 56,7 |
| | De acuerdo | 11 | 36,7 | 36,7 | 93,3 |
| | Totalmente de acuerdo | 2 | 6,7 | 6,7 | 100,0 |
| | Total | 30 | 100,0 | 100,0 | |

Del total de 30 encuestados, 12 de los entrevistados se manifestaron en no estar ni de acuerdo ni en desacuerdo sobre la viabilidad de concretarse acciones antijurídicas contra los datos y sistemas informáticos en OSITRAN, a pesar de estar implementándose su plan de gobierno digital. Esto representa el 40% del total.

*Figura 2*

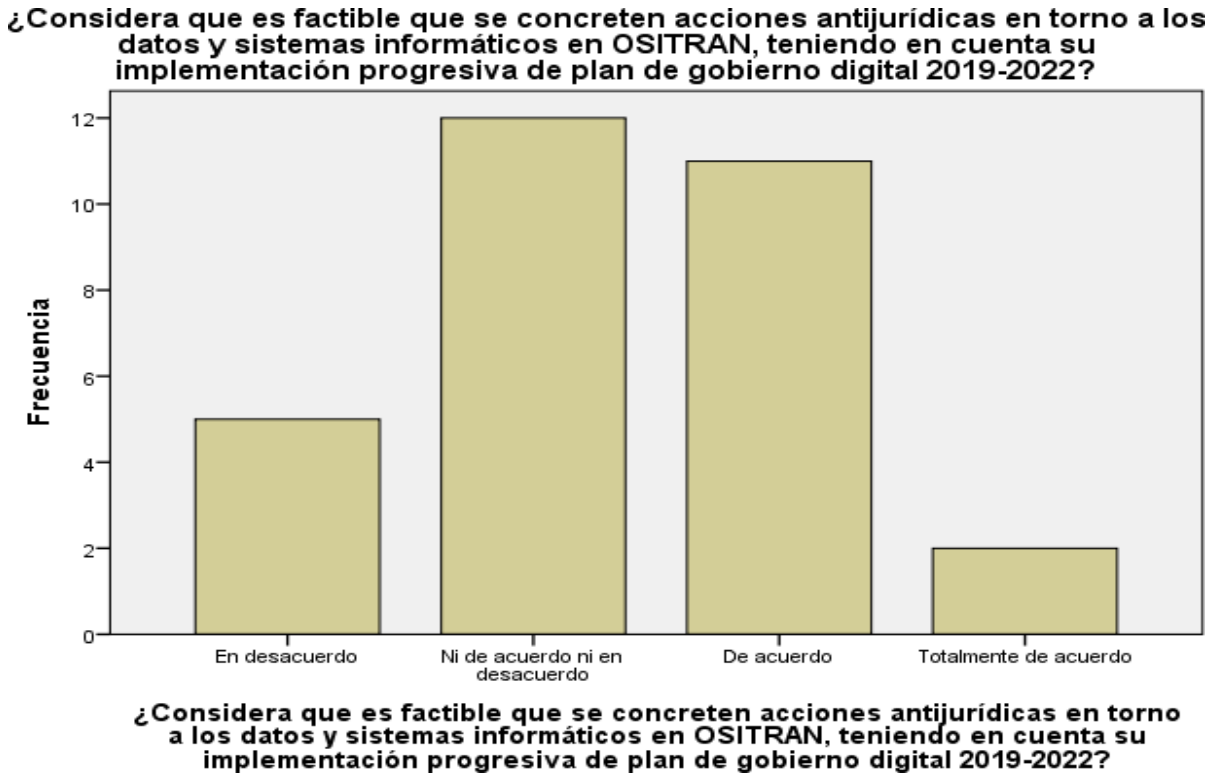



*Tabla 2*

**¿Cree usted que es viable que se concreten acciones antijurídicas que afecten el patrimonio informático de OSITRAN, teniendo en cuenta su implementación progresiva de plan de gobierno digital 2019-2022?**

| | | Frecuencia | Porcentaje | Porcentaje válido | Porcentaje acumulado |
|---|---|---|---|---|---|
| Válidos | En desacuerdo | 5 | 16,7 | 16,7 | 16,7 |
| | Ni de acuerdo ni en desacuerdo | 7 | 23,3 | 23,3 | 40,0 |
| | De acuerdo | 17 | 56,7 | 56,7 | 96,7 |
| | Totalmente de acuerdo | 1 | 3,3 | 3,3 | 100,0 |
| | Total | 30 | 100,0 | 100,0 | |

Del total de 30 encuestados, 17 se mostraron a favor de que se concreten acciones antijurídicas que afecten el patrimonio informático de OSITRAN, teniendo en cuenta la implementación progresiva de su plan de gobierno digital. Esto representa el 56,7% del total.

***Figura 3***

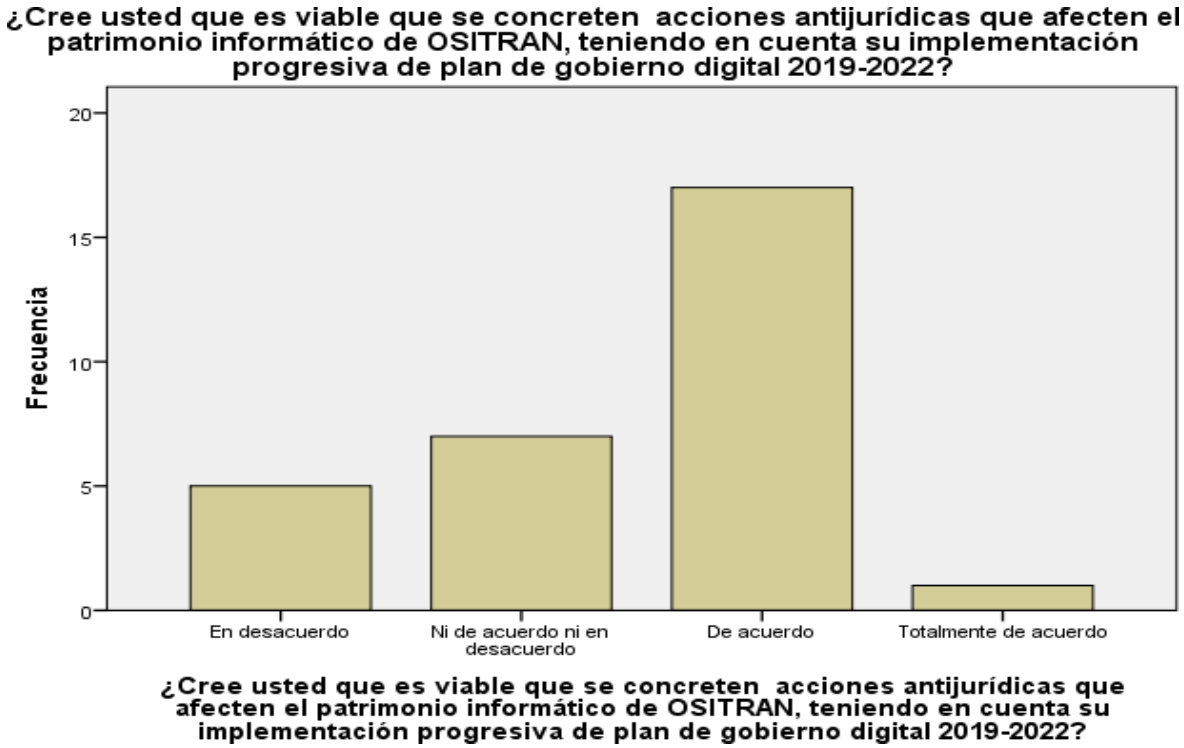


*Tabla 3*

**¿Considera que es esperable que se concreten acciones antijurídicas que atenten contra la fe pública informática, teniendo en cuenta su implementación progresiva de plan de gobierno digital 2019-2022?**

| | | Frecuencia | Porcentaje | Porcentaje válido | Porcentaje acumulado |
|---|---|---|---|---|---|
| Válidos | En desacuerdo | 8 | 26,7 | 26,7 | 26,7 |
| | Ni de acuerdo ni en desacuerdo | 5 | 16,7 | 16,7 | 43,3 |
| | De acuerdo | 15 | 50,0 | 50,0 | 93,3 |
| | Totalmente de acuerdo | 2 | 6,7 | 6,7 | 100,0 |
| | Total | 30 | 100,0 | 100,0 | |

De los 30 encuestados, 15 expresaron estar de acuerdo en torno a que puedan desarrollarse acciones antijurídicas que atenten contra la fe pública informática dotada por OSITRAN, a pesar de que la misma viene implementando su proyecto de gobierno digital 2019-2022. Esto representa el 50% del total.

*Figura 4*

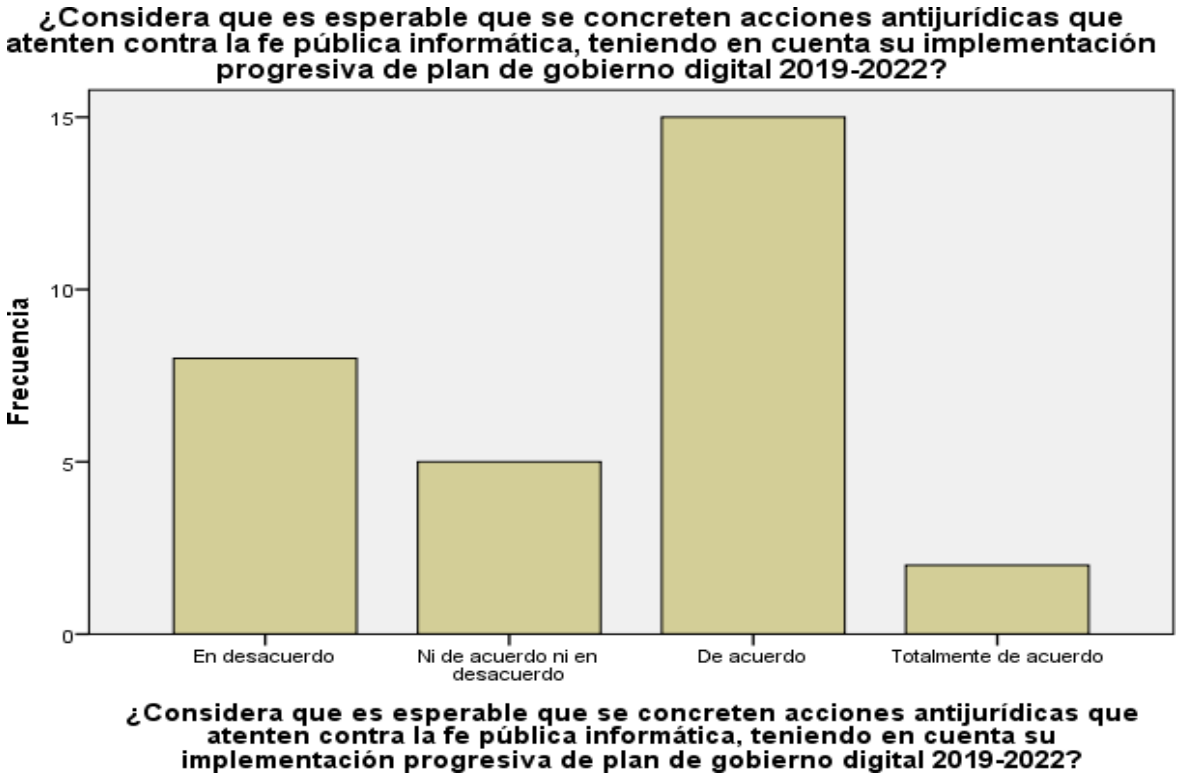



*Tabla 4*

**¿Cree usted que la supuesta eliminación de información de relevancia pública de OSITRAN u otro acontecimiento similar futuro puede constituir una amenaza a la ciber-seguridad nacional?**

| | | Frecuencia | Porcentaje | Porcentaje válido | Porcentaje acumulado |
|---|---|---|---|---|---|
| Válidos | En desacuerdo | 5 | 16,7 | 16,7 | 16,7 |
| | Ni de acuerdo ni en desacuerdo | 9 | 30,0 | 30,0 | 46,7 |
| | De acuerdo | 13 | 43,3 | 43,3 | 90,0 |
| | Totalmente de acuerdo | 3 | 10,0 | 10,0 | 100,0 |
| | Total | 30 | 100,0 | 100,0 | |

De los 30 encuestados, 13 se mostraron en favor de señalar que la supuesta supresión de información de relevancia pública de la base de datos de OSITRAN u otro hecho similar puede calificarse como una eventual amenaza a la ciber-seguridad nacional. Esto representa el 43,3% del total.

***Figura 5***

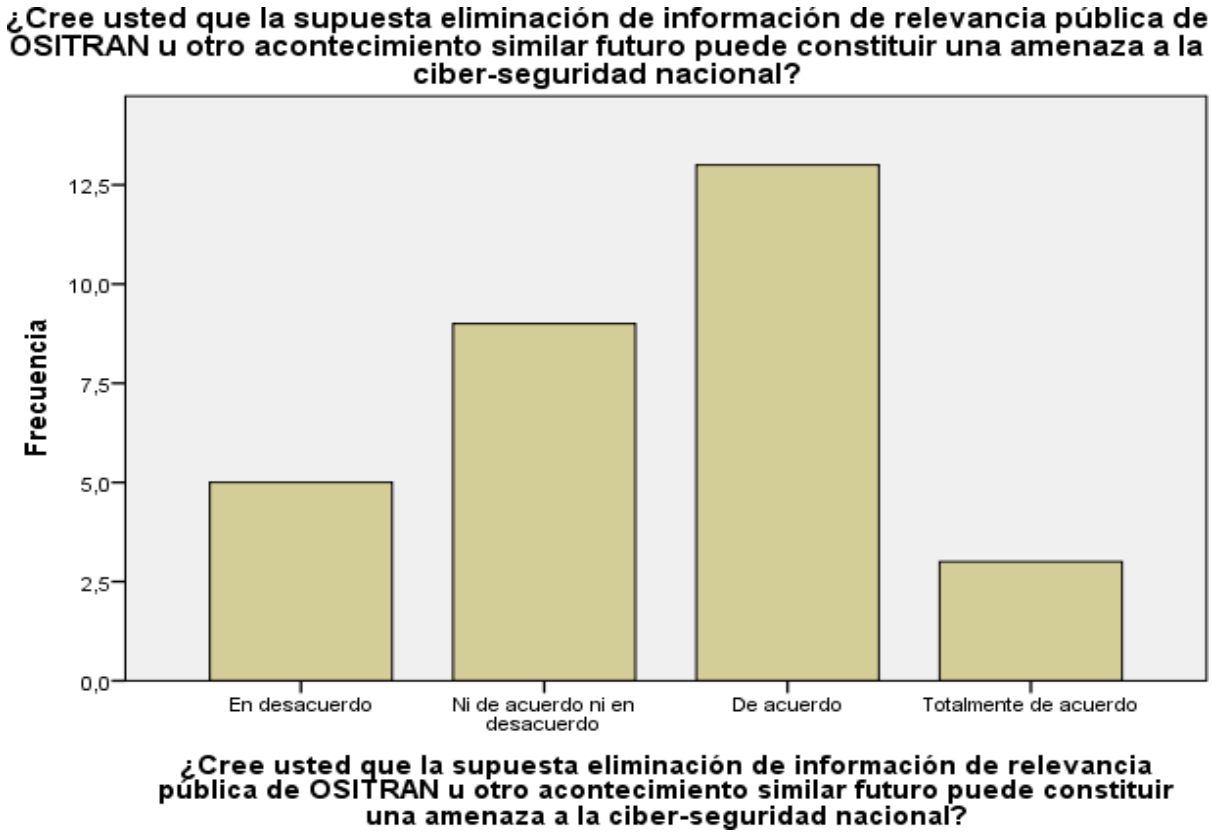


*Tabla 5*

**¿Considera que de producirse algún delito informático en el marco de un proyecto de gobierno digital de alguna entidad pública nos encontraremos ante una potencial amenaza a la ciber-seguridad?**

| | | Frecuencia | Porcentaje | Porcentaje válido | Porcentaje acumulado |
|---|---|---|---|---|---|
| Válidos | En desacuerdo | 5 | 16,7 | 16,7 | 16,7 |
| | Ni de acuerdo ni en desacuerdo | 9 | 30,0 | 30,0 | 46,7 |
| | De acuerdo | 13 | 43,3 | 43,3 | 90,0 |
| | Totalmente de acuerdo | 3 | 10,0 | 10,0 | 100,0 |
| | Total | 30 | 100,0 | 100,0 | |

De los 30 encuestados, 13 se mostraron en favor que de producirse un hipotético delito informático en una entidad pública que viene implementando su proyecto de gobierno digital, dicho suceso puede ubicarse en el campo de amenazas a la ciber-seguridad nacional. Esto representa el 43,3% del total.

*Figura 6*

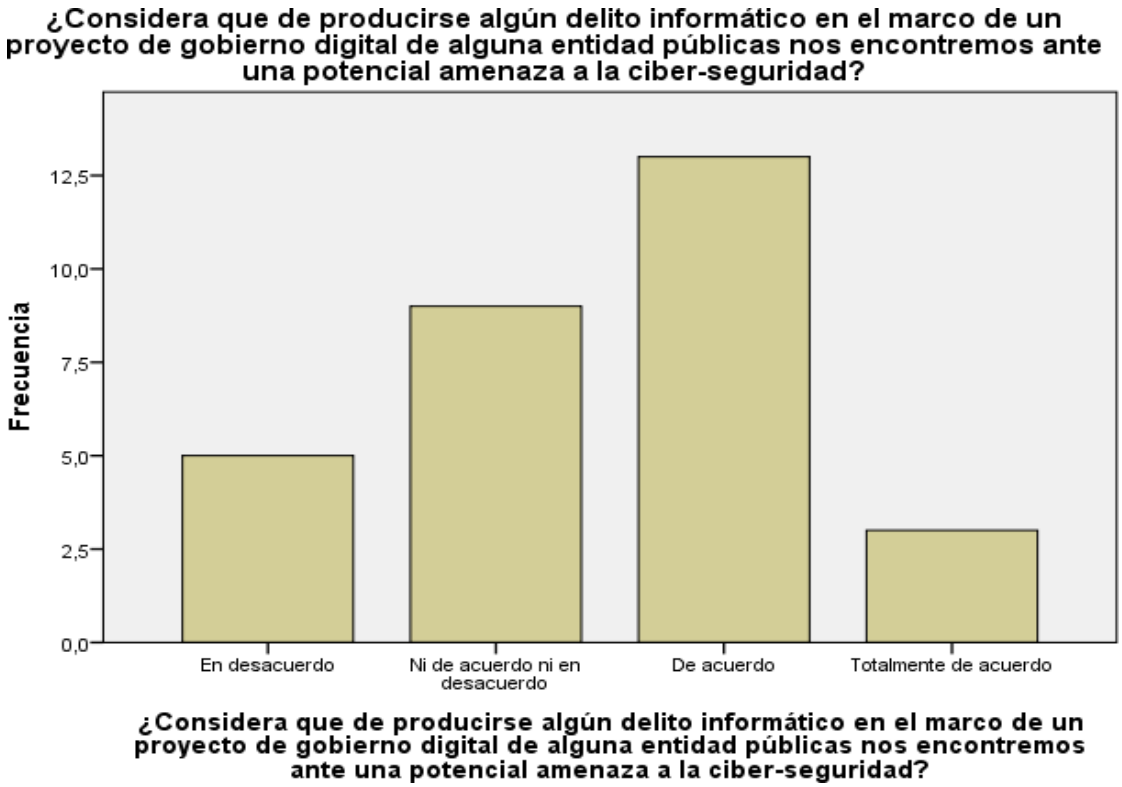



*Tabla 6*

**¿Piensa usted que los avances en materia de acciones antijurídicas digitales imponen a los Estados un mayor esfuerzo en materia de combatir las amenazas a la ciber-seguridad?**

| | | Frecuencia | Porcentaje | Porcentaje válido | Porcentaje acumulado |
|---|---|---|---|---|---|
| Válidos | En desacuerdo | 4 | 13,3 | 13,3 | 13,3 |
| | Ni de acuerdo ni en desacuerdo | 12 | 40,0 | 40,0 | 53,3 |
| | De acuerdo | 9 | 30,0 | 30,0 | 83,3 |
| | Totalmente de acuerdo | 5 | 16,7 | 16,7 | 100,0 |
| | Total | 30 | 100,0 | 100,0 | |

Del total de 30 encuestados, 12 expresaron no estar de acuerdo ni en desacuerdo en torno a que los avance en materia de acciones antijurídicas digitales imponen a los Estados un mayor esfuerzo en materia de combatir las amenazas a la ciber-seguridad. Esto representa el 40% del total.

***Figura 7***

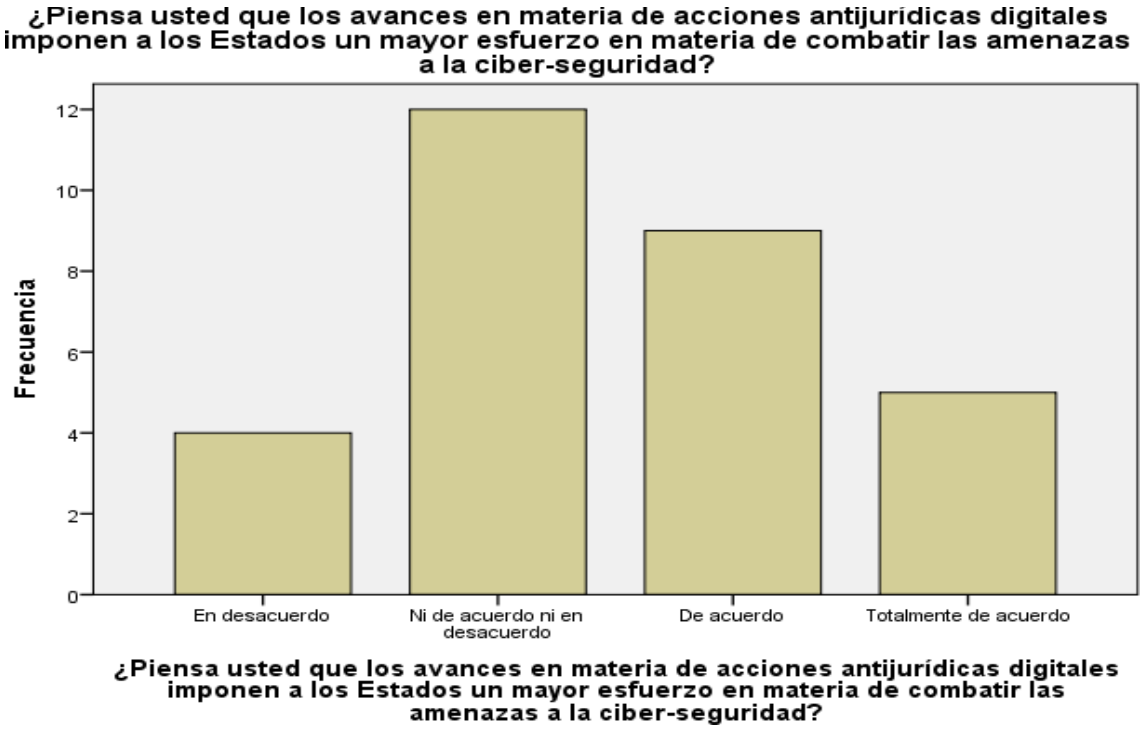


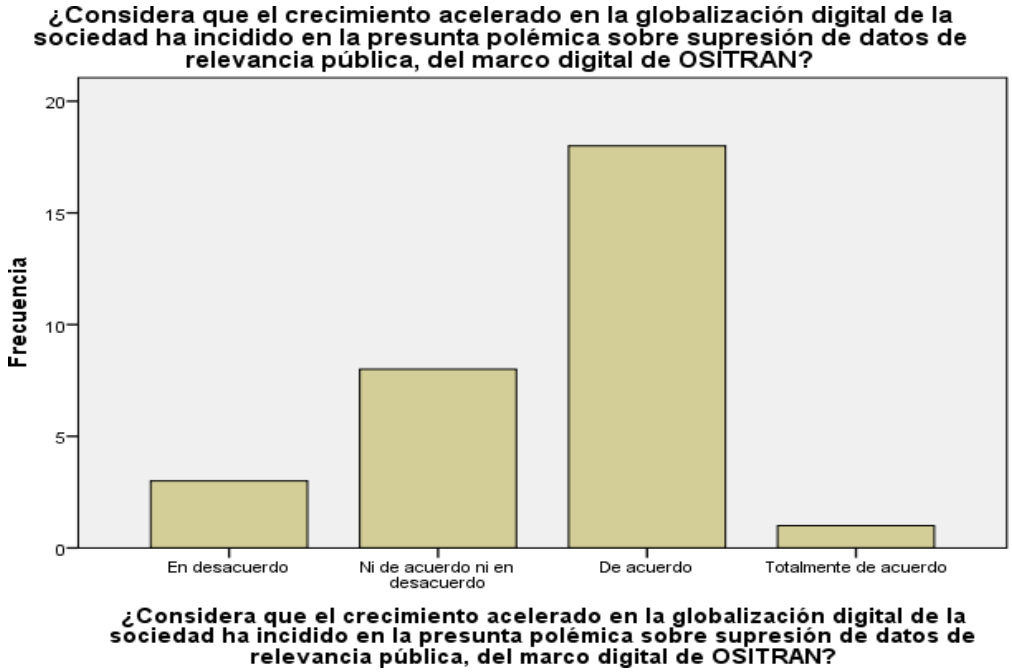
*Tabla 7*

**¿Considera que el crecimiento acelerado en la globalización digital de la sociedad ha incidido en la presunta polémica sobre supresión de datos de relevancia pública, del marco digital de OSITRAN?**

| | | Frecuencia | Porcentaje | Porcentaje válido | Porcentaje acumulado |
|---|---|---|---|---|---|
| Válidos | En desacuerdo | 3 | 10,0 | 10,0 | 10,0 |
| | Ni de acuerdo ni en desacuerdo | 8 | 26,7 | 26,7 | 36,7 |
| | De acuerdo | 18 | 60,0 | 60,0 | 96,7 |
| | Totalmente de acuerdo | 1 | 3,3 | 3,3 | 100,0 |
| | Total | 30 | 100,0 | 100,0 | |

Del total de 30 encuestados, 18 aludieron estar en favor de considerar que el crecimiento acelerado en la globalización digital de la sociedad ha incidido en la presunta polémica sobre supresión de datos de relevancia pública del marco digital de OSITRAN. Esto representa el 60% del total.

## *Figura 8*




## *Tabla 8*

**¿Piensa que los avances en materia de globalización digital de la sociedad han propiciado un fortalecimiento de los cursos de acción de los delitos informáticos?**

| | | Frecuencia | Porcentaje | Porcentaje válido | Porcentaje acumulado |
|---|---|---|---|---|---|
| Válidos | En desacuerdo | 5 | 16,7 | 16,7 | 16,7 |
| | Ni de acuerdo ni en desacuerdo | 13 | 43,3 | 43,3 | 60,0 |
| | De acuerdo | 9 | 30,0 | 30,0 | 90,0 |
| | Totalmente de acuerdo | 3 | 10,0 | 10,0 | 100,0 |
| | Total | 30 | 100,0 | 100,0 | |

Del total de 30 encuestados, 13 señalaron no estar de acuerdo ni en desacuerdo respecto a que los avances en materia de globalización digital de la sociedad han propiciado un fortalecimiento de los cursos de acción de los delitos informáticos. Esto representa el 43,3% del total.

***Figura 9***

*Tabla 9*

**¿Cree usted que los Estados deben adoptar medidas para retener el avance de la globalización digital de la sociedad, a fin de combatir los delitos informáticos?**

| | | Frecuencia | Porcentaje | Porcentaje válido | Porcentaje acumulado |
|---|---|---|---|---|---|
| Válidos | En desacuerdo | 2 | 6,7 | 6,7 | 6,7 |
| | Ni de acuerdo ni en desacuerdo | 8 | 26,7 | 26,7 | 33,3 |
| | De acuerdo | 17 | 56,7 | 56,7 | 90,0 |
| | Totalmente de acuerdo | 3 | 10,0 | 10,0 | 100,0 |
| | Total | 30 | 100,0 | 100,0 | |

Del total de 30 encuestados, 17 compartieron su parecer de estar de acuerdo en torno a que los Estados deben adoptar medidas para retener el avance de la globalización digital de la sociedad, a fin de combatir los delitos informáticos. Esto representa el 56,7% del total.

*Figura 10*

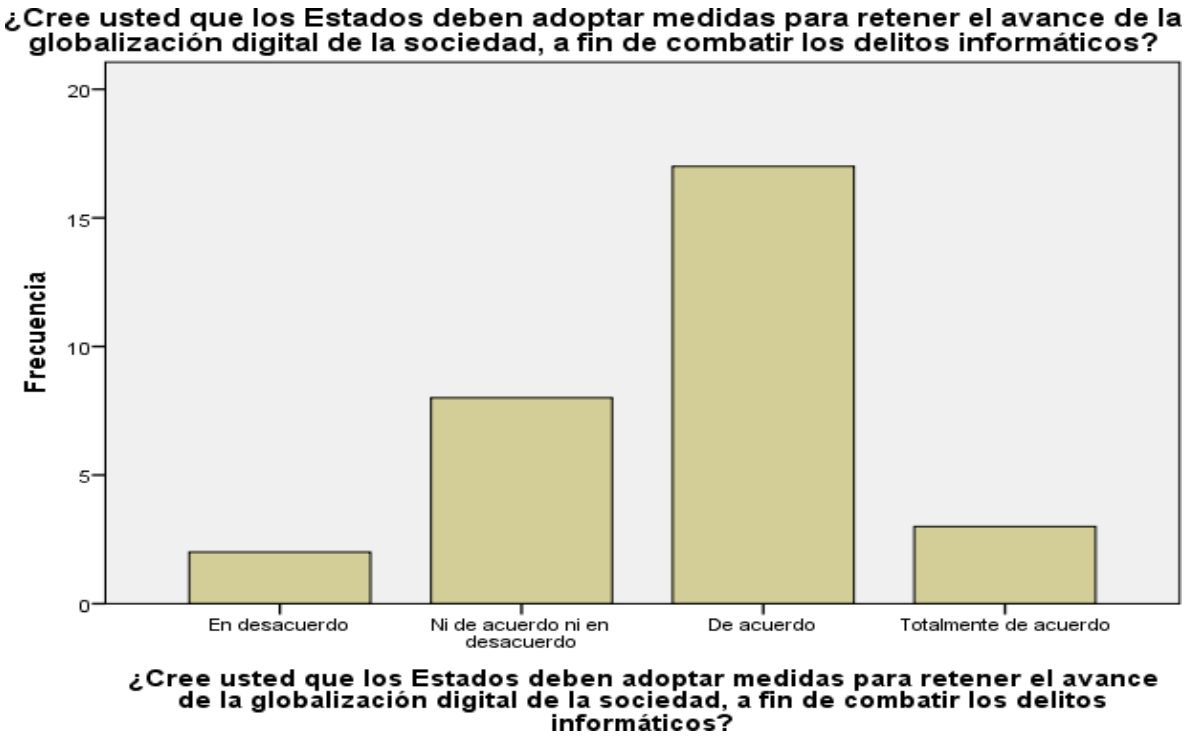



*Tabla 10*

**¿Considera que los actuales usos de las tecnologías de la información y de la comunicación son consistentes con los propósitos de los gobiernos digitales?**

| | | Frecuencia | Porcentaje | Porcentaje válido | Porcentaje acumulado |
|---|---|---|---|---|---|
| Válidos | En desacuerdo | 11 | 36,7 | 36,7 | 93,3 |
| | Ni de acuerdo ni en desacuerdo | 9 | 30,0 | 30,0 | 56,7 |
| | De acuerdo | 8 | 26,7 | 26,7 | 26,7 |
| | Totalmente de acuerdo | 2 | 6,7 | 6,7 | 100,0 |
| | Total | 30 | 100,0 | 100,0 | |

Del total de 30 encuestados, 11 expresaron estar en desacuerdo respecto a que los actuales usos de las tecnologías de la información y de la comunicación son consistentes con los propósitos de los gobiernos digitales. Esto representa el 36,7% del total.

***Figura 11***

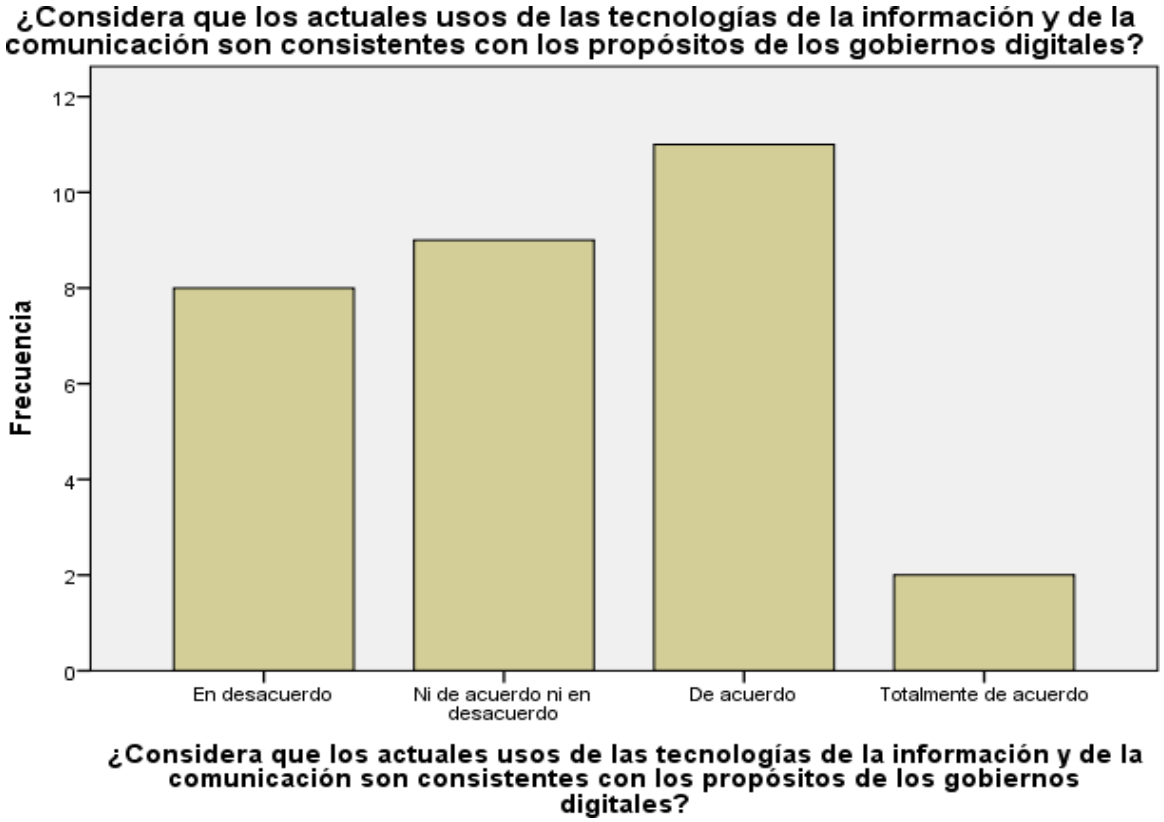


***Tabla 11***

**¿Cree usted que es necesario una reforma del Decreto Legislativo N°1412, respecto al manejo de las TICS, a fin de combatir de una mejor forma los delitos informáticos?**

| | | Frecuencia | Porcentaje | Porcentaje válido | Porcentaje acumulado |
|---|---|---|---|---|---|
| Válidos | En desacuerdo | 4 | 13,3 | 13,3 | 13,3 |
| | Ni de acuerdo ni en desacuerdo | 10 | 33,3 | 33,3 | 46,7 |
| | De acuerdo | 15 | 50,0 | 50,0 | 96,7 |
| | Totalmente de acuerdo | 1 | 3,3 | 3,3 | 100,0 |
| | Total | 30 | 100,0 | 100,0 | |

Del total de 30 encuestados, 15 refirieron estar en favor de que es necesario una reforma del Decreto Legislativo N°1412, respecto al manejo de las TICS, a fin de combatir de una mejor forma los delitos informáticos. Esto representa el 50% del total.

*Figura 12*

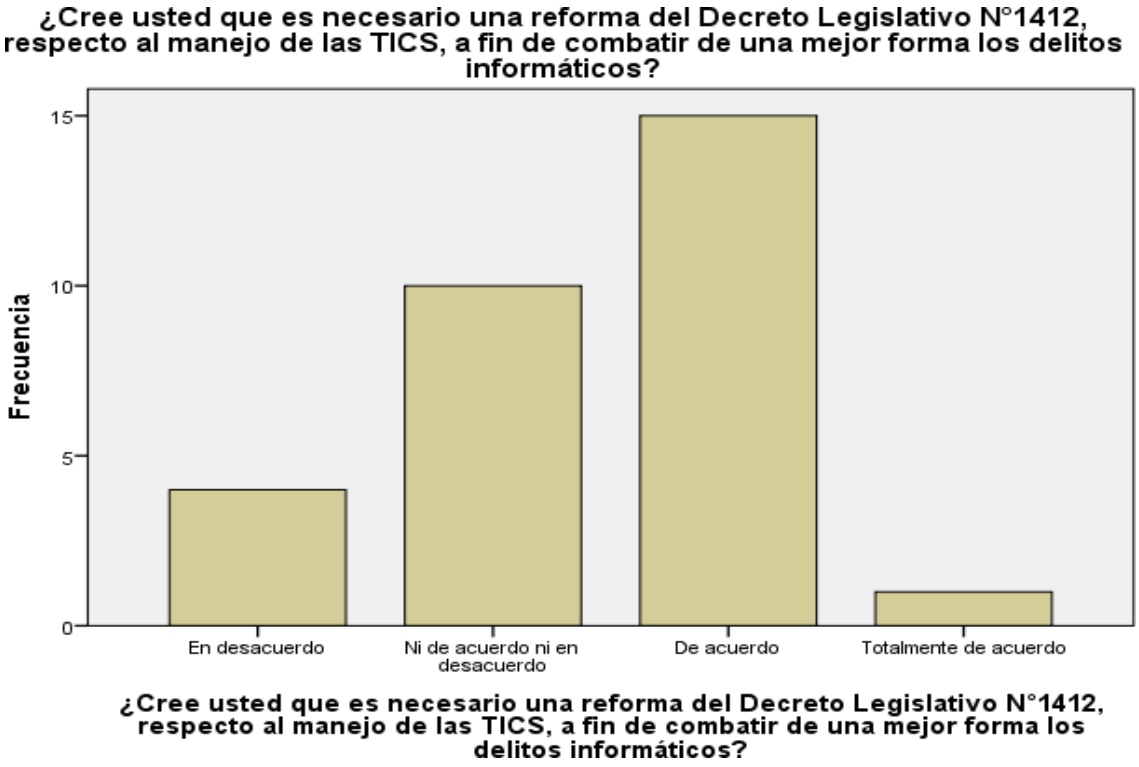



*Tabla 12*

**¿Piensa que las TICS se aplican como mecanismos eficaces y eficientes para efectivizar los planes de gobierno digital 2019-2022 de OSITRAN y otras instituciones públicas?**

| | | Frecuencia | Porcentaje | Porcentaje válido | Porcentaje acumulado |
|---|---|---|---|---|---|
| Válidos | En desacuerdo | 10 | 33,3 | 33,3 | 33,3 |
| | Ni de acuerdo ni en desacuerdo | 10 | 33,3 | 33,3 | 66,7 |
| | De acuerdo | 9 | 30,0 | 30,0 | 96,7 |
| | Totalmente de acuerdo | 1 | 3,3 | 3,3 | 100,0 |
| | Total | 30 | 100,0 | 100,0 | |

Del total de 30 encuestados, se visualizó que 10 personas se encuentran en desacuerdo de pensar que las TICS se aplican como mecanismos eficaces y eficientes para efectivizar los planes de gobierno digital 2019-2022 de OSITRAN y otras instituciones públicas. Esto representa el 33,3% del total.

***Figura 13***

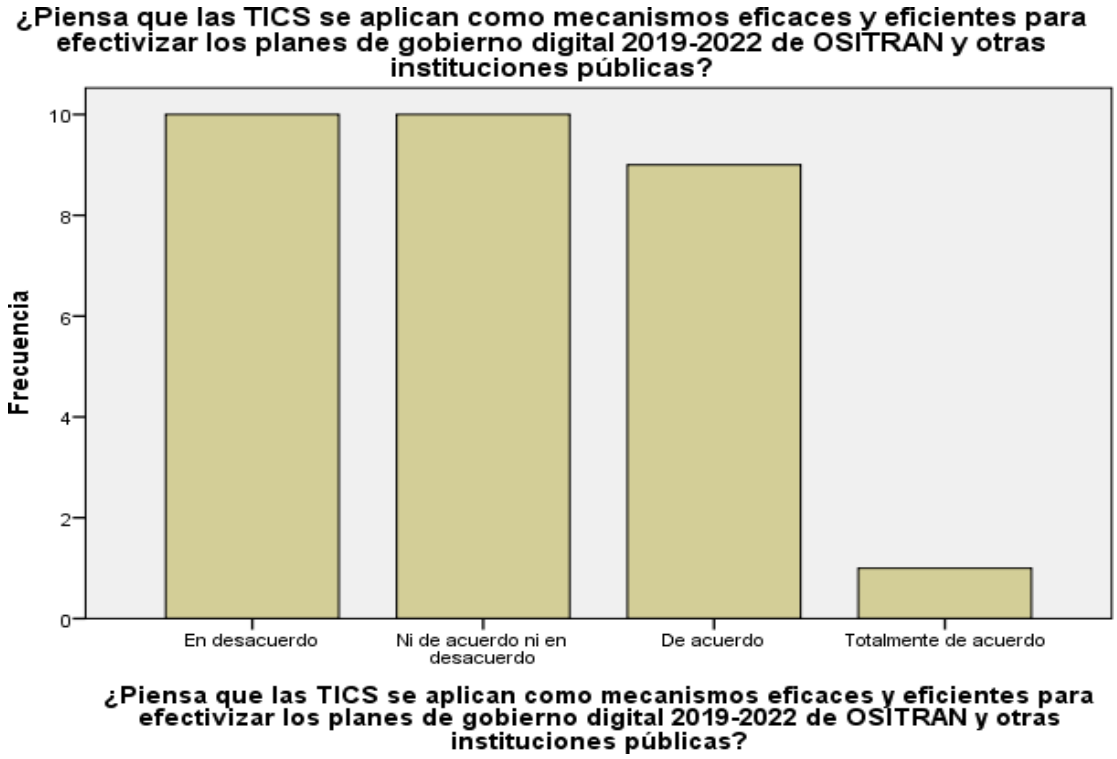


*Tabla 13*

**¿Piensa que la normativa nacional de gobierno digital dispone en la práctica, como prioridad, el objetivo de la creación de valor público?**

| | | Frecuencia | Porcentaje | Porcentaje válido | Porcentaje acumulado |
|---|---|---|---|---|---|
| Válidos | En desacuerdo | 4 | 13,3 | 13,3 | 13,3 |
| | Ni de acuerdo ni en desacuerdo | 9 | 30,0 | 30,0 | 43,3 |
| | De acuerdo | 14 | 46,7 | 46,7 | 90,0 |
| | Totalmente de acuerdo | 3 | 10,0 | 10,0 | 100,0 |
| | Total | 30 | 100,0 | 100,0 | |

De un total de 30 encuestados, 14 consideran estar de acuerdo en lo que concierne a que la normativa nacional de gobierno digital dispone en la práctica, como prioridad, el objetivo de la creación de valor público. Esto representa el 46,7% del total.

*Figura 14*

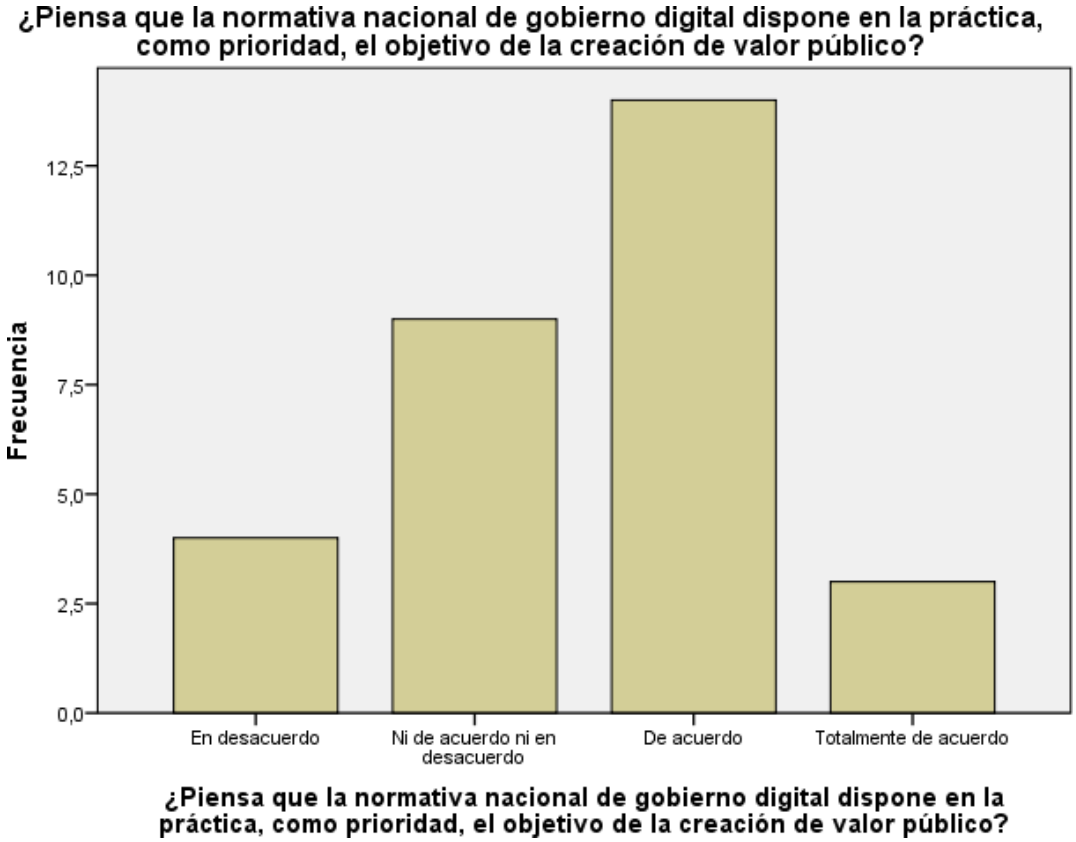



*Tabla 14*

**¿Cree usted que la normativa extranjera de gobierno digital dispone como prioridad, en la práctica, el objetivo de la creación de valor público?**

| | | Frecuencia | Porcentaje | Porcentaje válido | Porcentaje acumulado |
|---|---|---|---|---|---|
| Válidos | En desacuerdo | 6 | 20,0 | 20,0 | 20,0 |
| | Ni de acuerdo ni en desacuerdo | 12 | 40,0 | 40,0 | 60,0 |
| | De acuerdo | 7 | 23,3 | 23,3 | 83,3 |
| | Totalmente de acuerdo | 5 | 16,7 | 16,7 | 100,0 |
| | Total | 30 | 100,0 | 100,0 | |

De un total de 30 encuestados, 12 manifestaron no estar de acuerdo ni en desacuerdo respecto a que la normativa extranjera de gobierno digital dispone como prioridad, en la práctica, el objetivo de la creación de valor público. Esto representa el 40% del total.

***Figura 15***

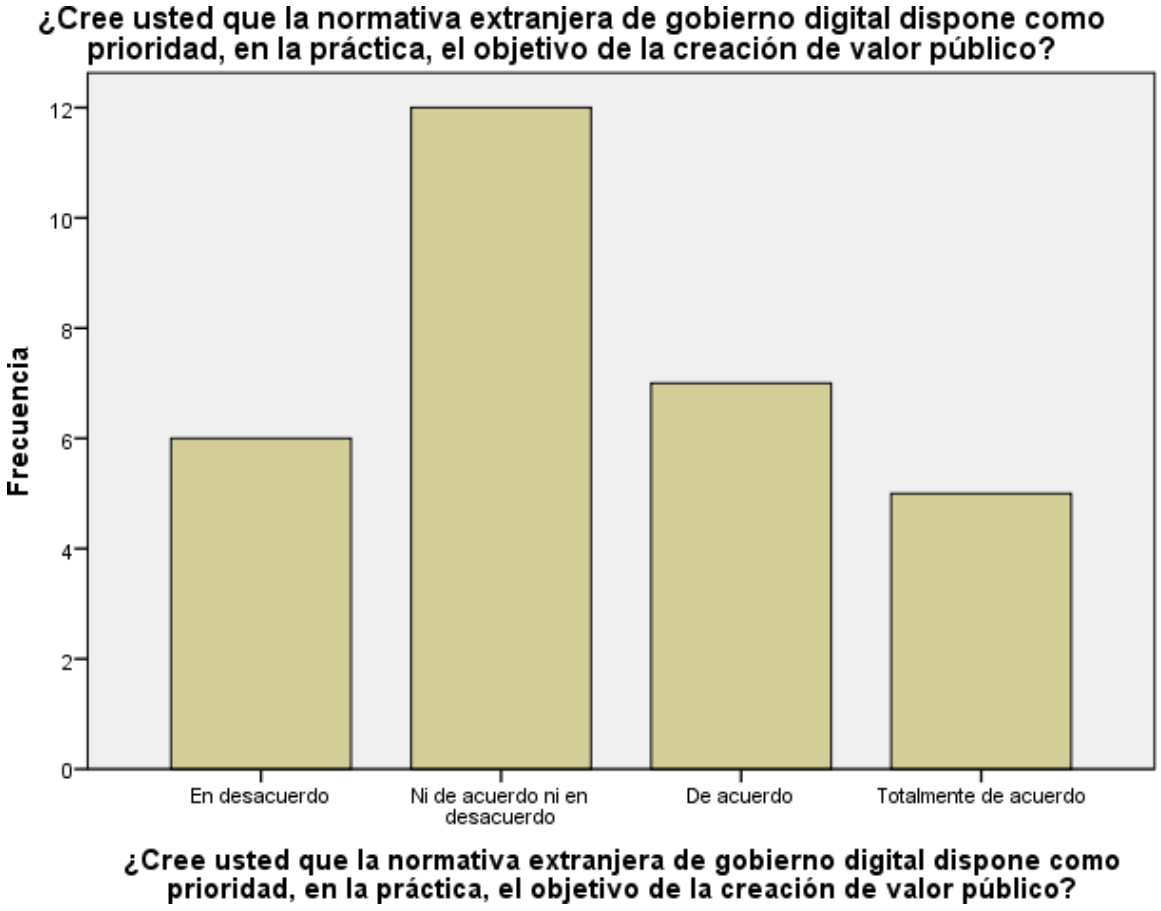


***Tabla 15***

**¿Considera que la creación de valor público en todo proyecto de gobierno digital se subordina al margen de legitimidad que posean las entidades de la administración pública?**

| | | Frecuencia | Porcentaje | Porcentaje válido | Porcentaje acumulado |
|---|---|---|---|---|---|
| Válidos | Totalmente en desacuerdo | 1 | 3,3 | 3,3 | 3,3 |
| | En desacuerdo | 5 | 16,7 | 16,7 | 20,0 |
| | Ni de acuerdo ni en desacuerdo | 6 | 20,0 | 20,0 | 40,0 |
| | De acuerdo | 16 | 53,3 | 53,3 | 93,3 |
| | Totalmente de acuerdo | 2 | 6,7 | 6,7 | 100,0 |
| | Total | 30 | 100,0 | 100,0 | |

De un total de 30 encuestados, 16 manifestaron estar de acuerdo respecto a que la creación de valor público en todo proyecto de gobierno digital se subordina al margen de legitimidad que posean las entidades de la administración pública. Esto representa el 53,3% del total.

*Figura 16*

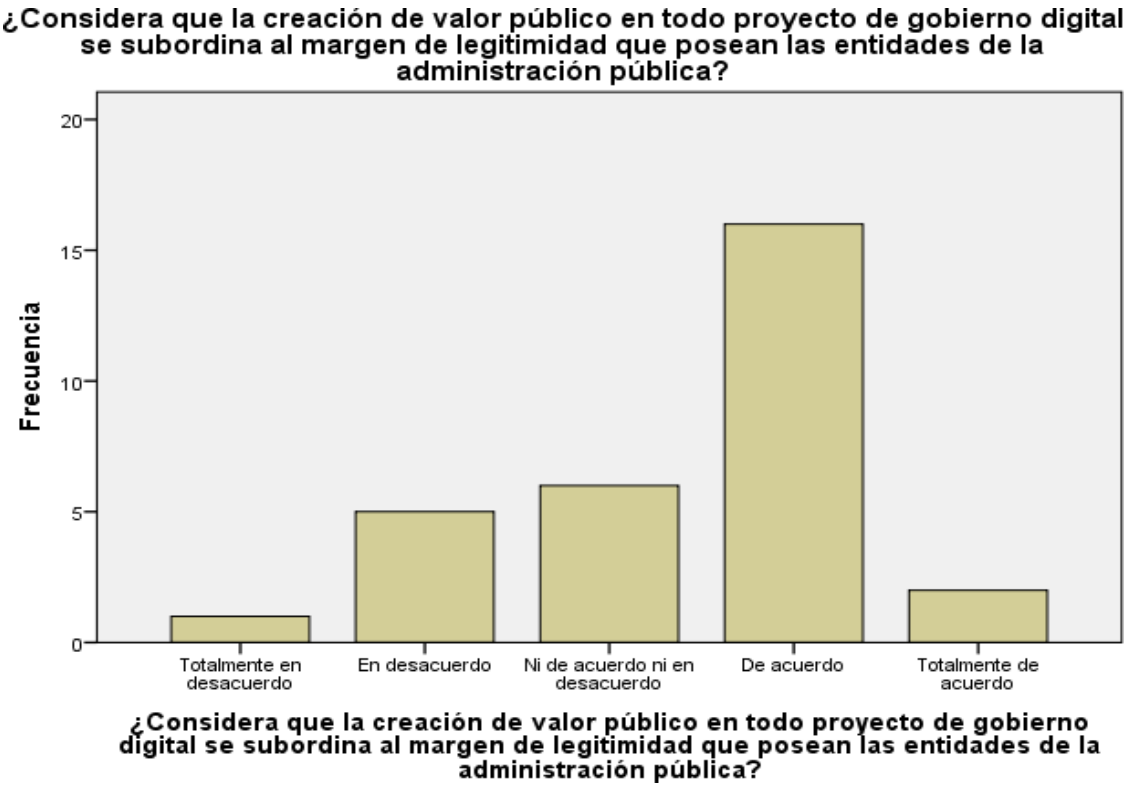



*Tabla 16*

**¿Considera que los avances del proyecto de gobierno digital de OSITRAN viabilizarán la concurrencia de un idóneo ecosistema digital en el futuro, si se tiene en cuenta el investigado hecho de supresión de información digital de relevancia pública de dicha entidad?**

| | | Frecuencia | Porcentaje | Porcentaje válido | Porcentaje acumulado |
|---|---|---|---|---|---|
| Válidos | En desacuerdo | 2 | 6,7 | 6,7 | 6,7 |
| | Ni de acuerdo ni en desacuerdo | 16 | 53,3 | 53,3 | 96,7 |
| | De acuerdo | 11 | 36,7 | 36,7 | 43,3 |
| | Totalmente de acuerdo | 1 | 3,3 | 3,3 | 100,0 |
| | Total | 30 | 100,0 | 100,0 | |

Del total de 30 encuestados, 16 consideran no estar de acuerdo ni en desacuerdo respecto a que los avances del proyecto de gobierno digital de OSITRAN viabilizarán la concurrencia de un idóneo ecosistema digital en el futuro, si se tiene en cuenta el investigado hecho de supresión de información digital de relevancia pública de dicha entidad. Esto representa el 53,3% del total.

***Figura 17***

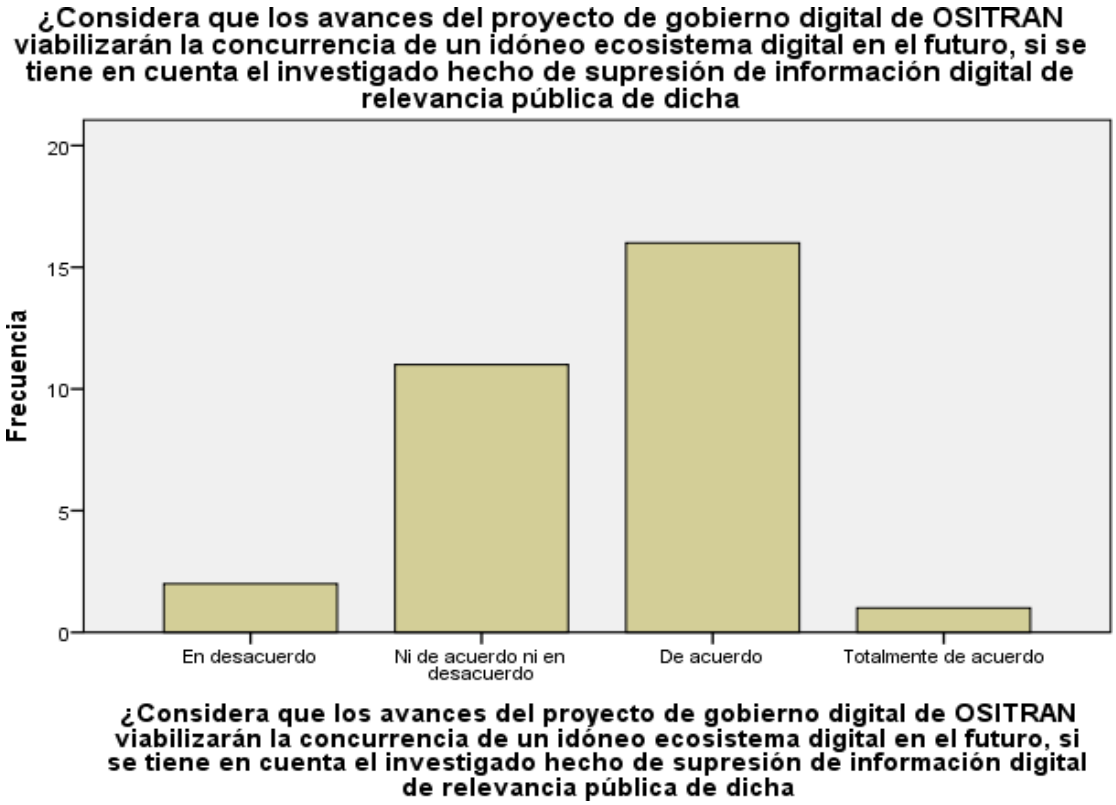


***Tabla 17***

**¿Piensa que las condiciones actuales en el marco de los proyectos de gobierno digital, en el ámbito extranjero, permiten hacer referencia a la presencia de un adecuado ecosistema digital?**

| | | Frecuencia | Porcentaje | Porcentaje válido | Porcentaje acumulado |
|---|---|---|---|---|---|
| Válidos | En desacuerdo | 6 | 20,0 | 20,0 | 20,0 |
| | Ni de acuerdo ni en desacuerdo | 10 | 33,3 | 33,3 | 53,3 |
| | De acuerdo | 10 | 33,3 | 33,3 | 86,7 |
| | Totalmente de acuerdo | 4 | 13,3 | 13,3 | 100,0 |
| | Total | 30 | 100,0 | 100,0 | |

Del total de 30 encuestados, se observa una división de 10 personas tanto para estar de acuerdo como para no estar de acuerdo ni en desacuerdo, respecto a que las condiciones actuales en el marco de los proyectos de gobierno digital, en el ámbito extranjero, permiten hacer referencia a la presencia de un adecuado ecosistema digital. Esto representa el 33,3% del total.

*Figura 18*

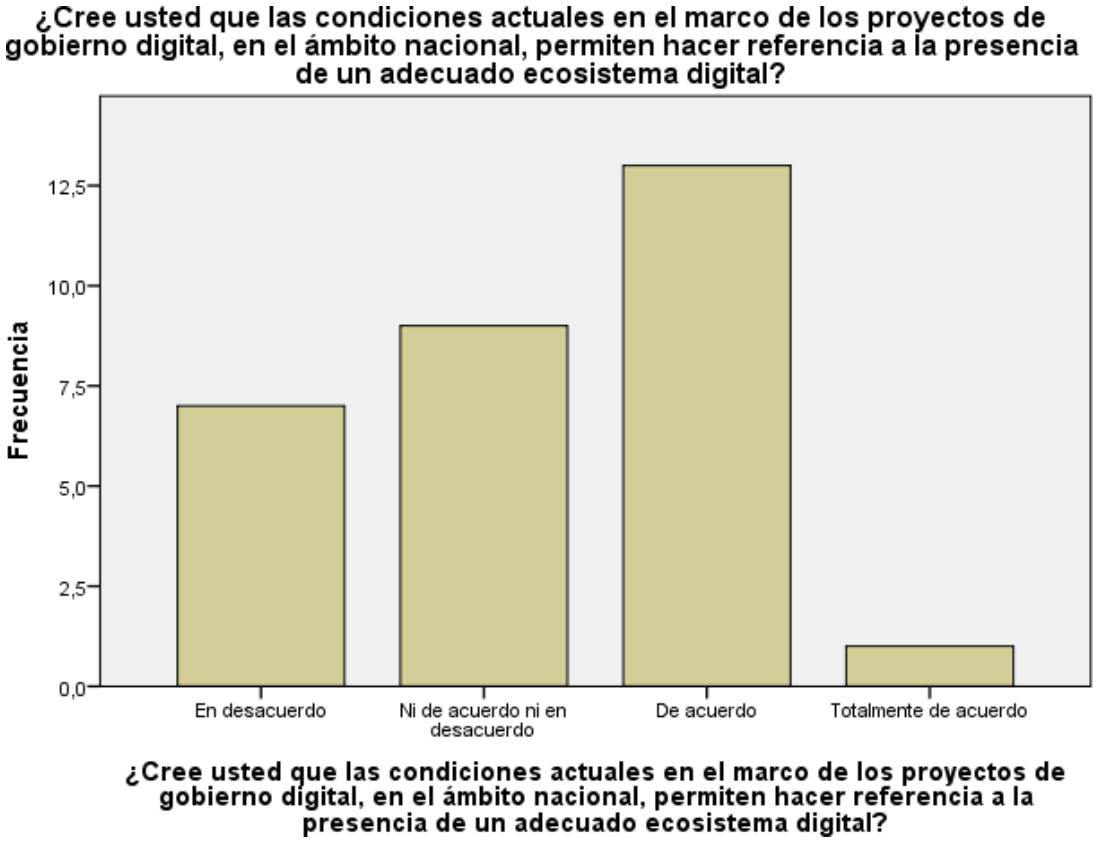

*Tabla 18*

**¿Cree usted que las condiciones actuales en el marco de los proyectos de gobierno digital, en el ámbito nacional, permiten hacer referencia a la presencia de un adecuado ecosistema digital?**

| | | Frecuencia | Porcentaje | Porcentaje válido | Porcentaje acumulado |
|---|---|---|---|---|---|
| Válidos | En desacuerdo | 13 | 43,3 | 43,3 | 96,7 |
| | Ni de acuerdo ni en desacuerdo | 9 | 30,0 | 30,0 | 53,3 |
| | De acuerdo | 7 | 23,3 | 23,3 | 23,3 |
| | Totalmente de acuerdo | 1 | 3,3 | 3,3 | 100,0 |
| | Total | 30 | 100,0 | 100,0 | |

De un total de 30 encuestados, 13 manifestaron encontrarse en desacuerdo respecto a que las condiciones actuales en el marco de los proyectos de gobierno digital, en el ámbito nacional, permiten hacer referencia a la presencia de un adecuado ecosistema digital. Esto representa el 43,3 % del total.

***Figura 19***




## Discusión

En función de los resultados surgidos a partir del instrumento de recopilación de datos, en base al planteamiento de la hipótesis principal, se constata que los delitos informáticos sí disponen de una incidencia negativa para la implementación progresiva del proyecto de gobierno digital 2019-2022 de OSITRAN. Si bien es cierto, que el respaldo a la hipótesis de la investigación ha

sido confirmada contundentemente, en lo que concierne al delito informático contra el patrimonio y la fe pública, a diferencia del atentado contra datos y sistemas informáticos (donde la opinión predominante fue una neutral, pero le sucedió en la alícuota de pareceres, el que sí afecta al plan de gobierno digital), es viable aseverar que la absolución de las incógnitas planteadas, en cuanto a estos 3 delitos informáticos en conjunto con otros aspectos adicionales (como la consideración de que el investigado hecho de supresión de información de relevancia nacional de la base digital de OSITRAN, la creencia en mayoría de que las TICS y el avance digital acelerado de la sociedad, han coadyuvado al fortalecimiento del curso de acción de los delitos informáticos, la aclamación de una reforma en los parámetros del DL N°1412, el dilema de poseer un adecuado ecosistema digital a raíz de los acontecimientos suscitados en OSITRAN, en el marco de insertar su proyecto de gobierno digital 2019-2022) conllevan a entender que los delitos informáticos sí han hecho acto de presencia e influencia en torno a las tratativas de OSITRAN, en su fin por implementar un proyecto de gobierno digital, por lo que no es desproporcional pensar que así como los delitos informáticos (en las 3 clases citadas) han tenido implicancias en el marco de gobierno digital de OSITRAN, los mismos puedan direccionarse para otros proyectos de gobierno digital 2019-2022, como en el caso de la OEFA, MINSA, entre otros actores de la administración pública.

Sin perjuicio de lo anterior, algunos detalles que no pueden hacerse a un lado es el proceso de contrastar algunos derivados del instrumento agrupador de datos, para con otras investigaciones científicas preexistentes. En específico, al progreso acelerado de la sociedad digital y su correlativo incremental de los delitos informáticos, el manejo inadecuado de las TICS como medio comisivo de delitos informáticos y el contexto de reforma normativa para combatir las ciber-amenazas.

Por ejemplo, en el caso de Morales (2016) su investigación estructuró, en función de un instrumento de recopilación de datos (encuesta) y el procesamiento de datos mediante el programa

SPS, un modelo donde el cual las apreciaciones vertidas en su sección “conclusiones” se contrastaran con las sub-hipótesis del trabajo, siendo una de tales apreciaciones lo relativo a que la problemática de la Delincuencia Informática ha sido dificultoso en razón de un exorbitante y célere avance de la tecnología informática, de modo tal que dichos avances se vieron reflejados en los medios computacionales utilizados por la delincuencia. El punto de comparación con los resultados de nuestra investigación es que tanto el estudio de Morales como el nuestro se centra en la coincidencia de pareceres en referencia a la elevación de la tasa de delitos informáticos, producto de la mejoría exasperada de la sociedad digital.

De otro lado, en lo que concierne a los inadecuados empleos de las TICS para la concreción de delitos informáticos, es plenamente concordante con nuestros resultados lo señalado por Alejo (2018), quien para cotejar su propuesta de hipótesis, elaboró y transcribió una entrevista al especialista ecuatoriano Santiago Acurio, siendo el parecer expuesto que tanto el uso como la aparición de nuevas tecnologías de información y comunicación ha permitido que la ciencia y tecnología también avance, pero así mismo lo mal utilizan como un factor criminal permitiendo la creación de nuevas modalidades delictivas.

Por último, cabe recordar que los frutos obtenidos en nuestro instrumento de recopilación de datos arrojaron una aceptación mayoritaria en cuanto es necesario una reforma del DL N°1412, en la sección relativa a las TICS, para combatir las acciones antijurídicas informáticas; sin embargo, a criterio de Zorrilla (2018), el problema de afrontar las apariciones incesantes de los delitos informáticos se centra no en modificar el DL N°1412, sino la ley de delitos informáticos (N°30096), basando su conclusión en que los resultados de sus respectivos mecanismos de recopilación de datos conceptúan que un 83,3% de los encuestados aluden que la ley de delitos informáticos presenta una serie de inconsistencias normativas, lo cual se habría producido por su

modificatoria Ley N°30171, al referir un 60% de la comunidad encuestada que las deficiencias normativas de la primigenia ley de delitos informáticos fueron solucionadas por esta norma modificatoria.

## Conclusiones

Se ha podido comprobar que los delitos informáticos (en su variante de atentando contra los datos y sistemas informáticos, fraude informáticos y contra la fe pública informática) sí se encuentran provistos de una incidencia negativa para los propósitos de ingreso al sistema jurídico del proyecto de gobierno digital de OSITRAN 2019-2022, en función de las particularidades del aún investigado suceso de supresión de información de relevancia pública, de la base de datos de dicha entidad, por lo cual no es irrazonable suponer que los delitos informáticos puedan acaecer en otra entidad pública, a pesar de que la misma se encuentra en trámite de aplicar su proyecto de gobierno digital 2019-2022, como el caso de OSITRAN y OEFA.

Se debe señalar que se ha dejado en claro que los usos inadecuados de las Tecnologías de la Información (TICS), en conjunto con el raudo crecimiento de la sociedad digital, han permitido que el abanico de medios y estrategias se amplié para el delincuente informático, lo cual requiere ser analizado por el Estado a fin de estudiar las posibilidades, viabilidades, para afrontar estas situaciones indeseadas, aunque ya incorporadas a nuestro ordenamiento jurídico.

Es de manifestar que se ha podido verificar que la existencia de un ecosistema digital de gobierno adecuado e idóneo se encuentra condicionado a diversas aristas, aunque las principales son la preponderancia del objetivo de la creación de valor público por parte de las entidades públicas digitalizadas y el disponer de un modelo articulado y unificado para responder ante los cursos de acción antijurídica informática, ya sea si la misma se encuentra en un grado potencial o real.

## Recomendaciones

Se hace necesario que, en función de las eventuales manifestaciones de los delitos informáticos en los proyectos de gobierno digital y de los componentes del cuestionado e investigado suceso de supresión de información de relevancia pública del marco digital de OSITRAN, las indistintas entidades públicas que se encuentran en proceso de implementar su proyecto de gobierno digital (OSITRAN, OEFA, MINSA, etc) refuercen sus políticas y estándares de protección frente a los diferentes cursos de acción de los delitos informáticos, siendo un claro ejemplo el tema de las normas ISO, como bien lo propuso el esquema de gobierno digital de OSITRAN.

Se debe poner en conocimiento que, a raíz de las elevaciones de los casos que demuestran un manejo inoportuno de las TICS y el crecimiento ineficiente de las sociedad informáticas, es fundamental que los agentes gubernamentales en cooperación con la sociedad civil debidamente representada, adopten una mentalidad de planificar estratégicamente el cómo pueden combatir estas 2 situaciones indeseadas para un país específico, ya que si bien es importante la concurrencia de las TICS como un próspero crecimiento de la sociedad digital, ambos ideales deben realizarse en función de criterios de razonabilidad, eficiencia y de empleo óptimo.

Es importante dejar sentado que es necesario que la labor gubernamental para los próximos años, ya sea en materia de diálogo como de reformas normativas en materia digital, posea como su principal mentalidad la prosecución de generar valor público, mediante los diferentes medios informáticos provistos por las TICS, de manera tal que pueda generarse un marco idóneo, adecuado, con calidad, eficaz y eficiente, para la existencia del ecosistema digital de gobierno.

## Referencias

Acurio, S. (2015*). Derecho Penal Informático: Una visión general del Derecho Informático en el Ecuador con énfasis en las infracciones informáticas, la informática forense y la evidencia digital*. Guayaquil: S.E.

Aguilar, P. (2015). ¿Derecho informático o informática jurídica? *RITI*. 3 (6), pp.22-27.

Alarcón, D & Barrera, J. (2017). *Uso de internet y delitos informáticos en los estudiantes de primer semestre de la Universidad Pedagógica y Tecnológica de Colombia, Sede Seccional Sogamoso 2016*. (Tesis para obtener el grado de maestro). Lima, Universidad Privada Norbert Wiener.

Alfaro, R. & Bustos, G. & Gonzáles, A, & Loroño, J. (2005). *Introducción al Gobierno Electrónico: Actores y Dimensiones*. Valparaíso: Ediciones Universitarias de Valparaíso.

Arias-Flórez, M. & Daza-Martínez, L. & Ojeda-Pérez, J. & Rincón-Rodríguez, F. (2010). Delitos informáticos y entorno jurídico vigente en Colombia. Scielo. Recuperado de http://www.scielo.org.co/scielo.php?script=sci_arttext&pid=S0123-14722010000200003

Azaola, L. (2010). *Delitos informáticos y derecho penal.* México: Ubijus.

Canaris, C. (2015). Diferencia entre derecho informático e informática jurídica. S.L: Blogspot. http://carolcanaris22.blogspot.com/

Centro Latinoamericano de Administración para el desarrollo. (2007). Carta Iberoamericana de Gobierno Electrónico. (XVII Cumbre Iberoamericana, Chile). Recuperado de http://old.clad.org/documentos/declaraciones/cartagobelec.pdf/view

Certsuperior. (2015). Seguridad Digital. México, Lomas de Santa fe: Certsuperior. https://www.certsuperior.com/seguridad-digital/

Chávez, E. (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 para obtener el grado de doctor). Lima, Universidad Nacional Federico Villareal.

Código Penal de Argentina. Boletín Oficial de la República Argentina. Buenos Aires, Argentina. 29 de Octubre de 1921.

Código Penal Español. Boletín Oficial del Estado. Madrid, España. 24 de Noviembre de 1995.

Consejo de Europa. (2001). Convenio sobre la Ciber-delincuencia. (23.XI.2001). Recuperado de https://static.legis.pe/wp-content/uploads/2019/09/Convenio-sobre-la-Ciberdelincuencia-Legis.pe_.pdf

Cortez, A & Chang, C. (2015). *Diseño de un nuevo esquema para el procedimiento de indagación de los delitos informáticos.* (Tesis para obtener el título de ingeniero de sistemas). Guayaquil, Universidad Politécnica Salesiana.

Decreto N° 1008. Diario Oficial de Colombia. Bogotá, Colombia. 14 de Junio de 2018.

Decreto Legislativo N° 1412. Diario Oficial El Peruano. 12 de setiembre de 2018.

Delgado, L. (2014). Delitos informáticos- delitos electrónicos. México, Ciudad de México: Congreso de México. http://www.ordenjuridico.gob.mx/Congreso/pdf/120.pdf

Devia, E. (2016). *Delito informático: estafa informática del artículo 248.2 del código penal.* (Tesis para obtener el grado de doctor en derecho). Sevilla, Universidad de Sevilla.

Estrada, R. & Somellera, R. (1998). Delitos informáticos. *Dialnet.* Recuperado de https://dialnet.unirioja.es/descarga/articulo/248204.pdf

González, J. (2013). *Delincuencia Informática: daños informáticos del artículo 264 del código penal y propuesta de reforma.* (Tesis para obtener el grado de doctor). Madrid, Universidad Complutense de Madrid.

Gutiérrez, M. (1991). *Fraude informático y estafa.* Madrid: Ministerio de Justicia.

Kaspersky. (s.f) ¿Qué es la ciberseguridad? S.L: Kaspersky. https://latam.kaspersky.com/resource-center/definitions/what-is-cyber-security

Lara, M. & Pina, V. & Torres, L. (2013). El gobierno electrónico y la rendición de cuentas en la administración regional y estatal. *Scielo.* Recuperado de http://www.scielo.org.mx/scielo.php?script=sci_arttext&pid=S1405-10792013000400004

La Red, D. (2012). Teleprocesos y sistemas distribuidos: Monografía adscripción gobierno electrónico. Argentina, Buenos Aires: Universidad Nacional del Nordeste. http://exa.unne.edu.ar/informatica/SO/Monografia_Adscripcion_Gobierno_Electronico_Vera.pdf

Latina. (2019, noviembre 18). Desaparece información de testigos de caso chinchero. [Archivo de video]. Recuperado de https://www.youtube.com/watch?v=C6Tyu6cMLI0&t=383s

Ley de Gobierno Electrónico de la Ciudad de México. Gaceta Oficial del Distrito Federal. Ciudad de México, México. 07 de Octubre de 2015.

Ley N° 26.388. Boletín Oficial de la República Argentina. Buenos Aires, Argentina. 24 de Junio de 2008.

Ley N° 30096. Diario Oficial El Peruano. 21 de octubre de 2013.

Ley N° 30171. Diario Oficial El Peruano. 14 de marzo de 2014.

Ley N°39-2015. Boletín Oficial del Estado. Madrid, España. 02 de octubre de 2015.

Loredo, J. & Ramírez, A. (2013). Delitos informáticos: su clasificación y una visión general de las medidas de acción para combatirlo. *Celerinet.* Recuperado de http://eprints.uanl.mx/3536/1/Delitos_informaticos.pdf

Malvaez, A. (2008). Derecho informático e informática jurídica. México, Ciudad de México: Blogcindario. https://informaticajuridica.blogcindario.com/2008/10/00006-derecho-informatico-e-informatica-juridica.html

Martínez, G. & Riascos, S. & Solano, O. (2008). El gobierno electrónico como estrategia de participación ciudadana en la administración pública en Suramérica. Casos Colombia y Uruguay. *Libre empresa.* Recuperado de https://www.researchgate.net/publication/283051771_El_Gobierno_Electronico_como_estrategia_de_participacion_ciudadana_en_la_Administracion_publica_a_nivel_de_Suramerica-Casos_Colombia_y_Uruguay

MINTIC. (s.f) ¿Qué es la política de Gobierno Digital? Colombia, Bogotá: Gobierno en línea. https://estrategia.gobiernoenlinea.gov.co/623/w3-propertyvalue-7650.html

Montaño, J. & Saavedra, C. & Saavedra, C. (2018). Relación entre informática jurídica y el derecho informático. Herramientas básicas para los profesionales del derecho y de la informática. *Atlante.* Recuperado de https://www.eumed.net/rev/atlante/2018/11/informatica-juridica-derecho.html

Morales, D. (2016). *La inseguridad al utilizar los servicios de redes sociales y la problemática judicial para regular los delitos informáticos en el Perú-2015.* (Tesis para obtener el título de abogado). Pimentel, Universidad Señor de Sipán.

Naser, A. (s.f). Gobierno electrónico y Gestión pública. [Diapositivas de PowerPoint]. Recuperado 21 de agosto de 2018 de https://www.cepal.org/ilpes/noticias/paginas/5/39255/gobierno_electronico_anaser.pdf

OSITRAN. (2019). Plan de gobierno digital del OSITRAN 2019-2022. Perú, Lima: OSITRAN. https://www.ositran.gob.pe/wp-content/uploads/2019/05/023PD2019.pdf

Pardo, A. (2018). *Tratamiento jurídico penal de los delitos informáticos contra el patrimonio, Distrito Judicial de Lima, 2018.* (Tesis para obtener el grado de maestro). Lima, Universidad César Vallejo.

Peña, C. (s.f). Informática Jurídica y Derecho Informático. Argentina, Buenos Aires: Universidad de Palermo. https://www.palermo.edu/ingenieria/downloads/pdfwebc&T8/8CyT05.pdf

Rinaldi, P. (2017). ¿De dónde viene el delito cibernético? Origen y evolución del delito cibernético. S.L: Le vpn. https://www.le-vpn.com/es/delito-cibernetico-origen-evolucion/

Rodríguez, F. (2013). *Derecho informático. El derecho en la era digital. La sociedad de información y el sistema jurídico. Contratos informáticos. Protección jurídica de los programas de computación. Delitos informáticos. La tutela jurídica del sistema informático*. Buenos Aires: UNC

Ruiz, C. (2016). *Análisis de los delitos informáticos y su violación de los derechos constitucionales de los ciudadanos.* (Tesis para la obtención del título de abogado). Loja, Universidad Nacional de Loja.

Salvadori, I. (2013). La regulación de los daños informáticos en el código penal italiano. *Revista de Internet, Derecho y Política.* Recuperado de https://core.ac.uk/download/pdf/38996507.pdf

Terán, R. (2015). *La necesidad de incorporar en el código penal el tipo penal de falsificación informática.* (Tesis para obtener el título de abogado). La Paz, Universidad Mayor de San Andrés.

Universidad Internacional de Valencia. (s.f) ¿Qué es la seguridad informática y cómo puede ayudarme? España, Valencia: Universidad Internacional de Valencia. https://www.universidadviu.com/la-seguridad-informatica-puede-ayudarme/

Viega, J. (2011). Un nuevo desafío jurídico: Los delitos informáticos. Uruguay, Montevideo: Viega asociados.
http://mjv.viegasociados.com/wpcontent/uploads/2011/05/DelitosInformaticos.pdf

Villavicencio, F. (2014). Delitos informáticos. *Ius Et Veritas.* Recuperado de http://revistas.pucp.edu.pe/index.php/iusetveritas/article/view/13630

Zorrilla, K. (2018). *Inconsistencias y ambigüedades en la ley de delitos informáticos ley nº 30096 y su modificatoria ley nº 30171, que imposibilitan su eficaz cumplimiento*. (Tesis para obtener el título de abogado). Ancash, Universidad Nacional de Ancash.

# APÉNDICE N°1: INSTRUMENTO DE RECOPILACIÓN DE DATOS

| VARIABLES | Indicador | Preguntas | Totalmente de acuerdo | De acuerdo | Ni de acuerdo ni en desacuerdo | En desacuerdo | Totalmente en desacuerdo. |
|---|---|---|---|---|---|---|---|
| | | | 1 | 2 | 3 | 4 | 5 |
| **VARIABLE 1** | I1 **ACCIÓN ANTIJURÍDICA EN EL ENTORNO DIGITAL.** | 1. ¿Considera que es factible que se concreten acciones antijurídicas, en torno a los datos y sistemas informáticos en OSITRAN, teniendo en cuenta la implementación progresiva del plan de gobierno digital 2019-2022? | | | | | |
| | | 2. ¿Cree usted, que es viable que se concreten acciones antijurídicas que afecten el patrimonio informático de OSITRAN, teniendo en cuenta la implementación progresiva de plan de gobierno digital 2019-2022? | | | | | |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| **Delitos informáticos** | | 3. ¿Considera que es esperable que se concreten acciones antijurídicas que atenten contra la fe pública informática en las operaciones digitales con OSITRAN, teniendo en cuenta la implementación progresiva de plan de gobierno digital 2019-2022? | | | | | |
| | I2 **AMENAZA A LA CIBER-SEGURIDAD** | 1. ¿Cree usted que la supuesta eliminación de información de relevancia pública de OSITRAN u otro acontecimiento similar futuro puede constituir una amenaza a la ciber-seguridad nacional? | | | | | |
| | | 2. ¿Considera que de producirse algún delito informático en el marco de un proyecto de gobierno digital de alguna entidad públicas nos encontremos ante una potencial amenaza a la ciber-seguridad? | | | | | |
| | I3 **GLOBALIZACIÓN DIGITAL DE LA SOCIEDAD**. | 1. ¿Considera que el crecimiento acelerado en la globalización digital de la sociedad ha incidido en la presunta polémica sobre supresión de datos de relevancia pública, del marco digital de OSITRAN? | | | | | |
| | | 2. ¿Piensa que los avances en materia de globalización digital de la sociedad han propiciado un fortalecimiento de los cursos de acción de los delitos informáticos? | | | | | |
| | | 3. ¿Cree usted que los Estados deben adoptar medidas para retener el avance de la globalización digital de la sociedad, | | | | | |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | | a fin de combatir los delitos informáticos? | | | | | |
| **VARIABLE 2**<br><br>**Gobierno** | I1<br>**USO DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN.** | 1. ¿Considera que los actuales usos de las tecnologías de la información y de la comunicación son consistentes con los propósitos de los gobiernos digitales? | | | | | |
| | | 2. ¿Cree usted que es necesario una reforma del Decreto Legislativo N°1412, respecto al manejo de las TICS, a fin de combatir de una mejor forma los delitos informáticos? | | | | | |
| | | 3. ¿Piensa que las TICS se aplican como mecanismos eficaces y eficientes para efectivizar los planes de gobierno digital 2019-2022 de OSITRAN y otras instituciones públicas? | | | | | |
| | I2<br>**CREACIÓN DE VALOR PÚBLICO.** | 1. ¿Piensa que la normativa nacional de gobierno digital dispone en la práctica como prioridad, el objetivo de la creación de valor público? | | | | | |
| | | 2. ¿Cree usted que la normativa extranjera de gobierno digital dispone como prioridad, en la práctica el objetivo de la creación de valor público? | | | | | |
| | | 3. ¿Considera que la creación de valor público en todo proyecto de gobierno digital se subordina al margen de legitimidad que posean las entidades de la administración pública? | | | | | |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | I3<br>**ECOSISTEMA DIGITAL DE GOBIERNO** | 1. ¿Considera que los avances del proyecto de gobierno digital de OSITRAN viabilizarán la concurrencia de un idóneo ecosistema digital en el futuro, si se tiene en cuenta el investigado hecho de supresión de información digital de relevancia pública de dicha entidad y la sucesiva dación de delitos informáticos en el Perú? | | | | | |
| | | 2. ¿Piensa que las condiciones actuales en el marco de los proyectos de gobierno digital, en el ámbito extranjero, permiten hacer referencia a la presencia de un adecuado ecosistema digital? | | | | | |
| | | 3. ¿Cree usted que las condiciones actuales en el marco de los proyectos de gobierno digital, en el ámbito nacional, permiten hacer referencia a la presencia de un adecuado ecosistema digital? | | | | | |

## APÉNDICE N°2: MATRIZ DE CONSISTENCIA

**Título:** "La incidencia de los delitos informáticos en la implementación progresiva del plan de gobierno digital de OSITRAN 2019-2022".

| PROBLEMA | OBJETIVO | HIPÓTESIS | VARIABLES E INDICADORES | DIMENSIONES |
|---|---|---|---|---|
| **PROBLEMA PRINCIPAL**<br><br>¿Qué factores de los delitos informáticos inciden en la implementación progresiva del plan de gobierno digital de OSITRAN 2019-2022?<br><br>**PROBLEMAS ESPECÍFICOS**<br><br>**1.-** ¿En qué medida los delitos contra los datos y sistemas informáticos influyen en la implementación progresiva del plan de gobierno digital de OSITRAN 2019-2022?<br>**2.-** ¿De qué manera los delitos informáticos contra el patrimonio afectan en la implementación progresiva del plan de gobierno digital de OSITRAN 2019-2022?<br>**3.-** ¿De qué forma los delitos informáticos contra la fe pública repercuten en la implementación progresiva del plan de gobierno digital de OSITRAN 2019-2022? | **OBJETIVO GENERAL**<br><br>Determinar qué factores de los delitos informáticos inciden en la implementación progresiva del plan de gobierno digital de OSITRAN 2019-2022.<br><br>**OBJETIVOS ESPECÍFICOS**<br><br>**1.-** Determinar en qué medida los delitos contra los datos y sistemas informáticos influyen en la implementación progresiva del plan de gobierno digital de OSITRAN 2019-2022.<br>**2.-** Identificar de qué manera los delitos informáticos contra el patrimonio afectan en la implementación progresiva del plan de gobierno digital de OSITRAN 2019-2022.<br>**3.-** Verificar de qué forma los delitos informáticos contra la fe pública repercuten en la implementación progresiva del plan de gobierno digital de OSITRAN 2019-2022. | **HIPÓTESIS GENERAL**<br><br>Los delitos informáticos inciden negativamente en la implementación progresiva del plan de gobierno digital de OSITRAN 2019-2022.<br><br>**HIPÓTESIS SECUNDARIAS**<br><br>**1.-** Los delitos contra los datos y sistemas informáticos influyen negativamente en la implementación progresiva del plan de gobierno digital de OSITRAN 2019-2022.<br>**2.-** Los delitos informáticos contra el patrimonio afectan adversamente la implementación del plan de gobierno digital de OSITRAN 2019-2022.<br>**3.-** Los delitos informáticos contra la fe pública repercuten nefastamente en la implementación progresiva del plan de gobierno digital de OSITRAN 2019-2022. | **VARIABLE INDEPENDIENTE (X-1):**<br>Delitos informáticos.<br><br>**INDICADORES:**<br>**1.** Acción antijurídica en el entorno digital.<br>**2.** Amenaza a la seguridad digital<br>**3.** Producto de la globalización digital de la sociedad.<br><br>**VARIABLE DEPENDIENTE (Y-2):**<br>Gobierno digital.<br><br>**INDICADORES:**<br><br>**1.** Uso de tecnologías de la información y comunicación.<br>**2.** Creación de valor público.<br>**3.** Ecosistema digital de gobierno | **DIMENSIONES DE LOS DELITOS INFORMÁTICOS:**<br><br>1. Respuesta a los delitos informáticos durante sus inicios.<br>2. Respuesta a los delitos informáticos en la actualidad.<br><br>**DIMENSIONES DEL GOBIERNO DIGITAL:**<br><br>1. Claves de éxito del gobierno digital por el comportamiento de la administración pública.<br>2. Claves de éxito del gobierno digital por la colaboración ciudadana. |