Universidad Nacional Federico Villarreal

Vicerrectorado de INVESTIGACION

ESCUELA UNIVERSITARIA DE POSTGRADO

"LA CERTIFICACION DIGITAL Y LA GESTIÓN ADMINISTRATIVA EFICIENTE EN LAS INSTITUCIONES DEL ESTADO PERUANO"

TESIS PARA OPTAR EL GRADO ACADEMICO DE:

MAESTRO EN ADMINISTRACIÓN

AUTOR:
JUAN CARLOS HUGO RIOS BARRIOS

ASESOR:
EFRAIN JAIME GUARDIA HUAMANI

JURADOS:

Dr. AMBROSIO REYES, JORGE LUIS
Dr. RENGIFO LOZANO, RAUL ALBERTO
Dr. CUMPEN VIDAURRE, ROBERTO

LIMA - PERU
2018

Dedicatoria:

A Mis padres, por su constante apoyo y lecciones de cómo enfrentar con éxito las metas de la vida.

Agradecimientos:

A la Escuela de Postgrado de la UNFV, y a todos sus Docentes, por haberme dado la oportunidad de fortalecer mis conocimientos.

Al Dr. Jaime Guardia y a todos los revisores de mi tesis, por su colaboración no solo en la asesoría de Tesis, sino también por su valioso apoyo en la evolución de la presente investigación.

A todas las personas que me brindaron su valioso tiempo para el desarrollo de la presente investigación.

INDICE

RESUMEN

El presente trabajo de investigación titulado “La certificación digital y la gestión administrativa eficiente en las instituciones del estado peruano”, presenta un estudio y análisis de la relación existente entre la certificación digital y la gestión administrativa que permitiría mejorar la eficiencia de los procesos administrativos a través de la certificación digital en las instituciones del estado.

Para tal efecto dentro de la metodología de la investigación planteada, se utilizaron los siguientes métodos científicos: analíticos, inductivos, deductivos y descriptivos, entre otros. Considerando en dicha metodología el tipo, nivel, diseño, método, población, muestra, e instrumentos de recopilación de datos.

Después de realizar el análisis e interpretación de la prueba de campo, en concordancia con el desarrollo de los objetivos y de acuerdo a las hipótesis planteadas, se lograron demostrar mediante la contrastación y convalidación de las hipótesis lo siguiente:

- Que la variable independiente, la certificación digital, se relaciona con la variable dependiente, la gestión administrativa eficiente.
- La investigación ha podido determinar que el 75.15% de los encuestados realizan transacciones electrónicas bastante y regularmente. Asimismo, dedican semanalmente entre 4 a 6 horas de su tiempo en transacciones electrónicas (51.55%)

- Se ha logrado determinar que, el 84.47% de los encuestados manifiesta que siempre o casi siempre los mecanismos de protección de la certificación digital son seguros.
- Se estableció que, los encuestados consideran que siempre o casi siempre la certificación digital, permitiría una gestión administrativa eficiente, que incrementarían las transacciones electrónicas, y que difundir los mecanismos permitiría que más usuarios utilicen la certificación digital.
- El estudio demuestra que, el 75.78% de los encuestados manifiesta que la certificación digital agilizaría los trámites electrónicos que el sector privado realiza con el Estado. Asimismo, el 85.10% de los encuestados considera que la certificación digital reduciría los costos de las transacciones
- En conclusión, luego de haber contrastado las hipótesis planteadas y analizadas las tablas y gráficos elaborados en el cuestionario del trabajo de campo podemos afirmar que la certificación digital, permitiría una gestión administrativa eficiente en las instituciones del estado

Palabras Claves: Certificación digital, gestión administrativa, instituciones del estado, gestión eficiente, medios electrónicos.

ABSTRACT

This research paper entitled "Digital Certification and Efficient Administrative Management in Peruvian State Institutions" presents a study and analysis of the relationship between digital certification and administrative management that would improve the efficiency of administrative processes to Through digital certification in state institutions.

For this purpose, the following scientific methods were used: analytical, inductive, deductive and descriptive, among others. Considering in this methodology the type, level, design, method, population, sample, and instruments of data collection.

After performing the analysis and interpretation of the field test, in agreement with the development of the objectives and according to the hypotheses raised, they were able to demonstrate through the testing and validation of the hypotheses the following:

- That the independent variable, digital certification, is related to the dependent variable, efficient administrative management.
- Research has been able to determine that 75.15% of respondents conduct electronic transactions fairly and regularly. Also, they dedicate weekly between 4 to 6 hours of their time in electronic transactions (51.55%)
- It has been determined that 84.47% of the respondents say that the protection mechanisms of digital certification are always or almost always safe.

- It was established that respondents considered that digital certification would always or almost always allow efficient administrative management, which would increase electronic transactions, and that disseminating the mechanisms would allow more users to use digital certification.
- The study shows that 75.78% of the respondents stated that digital certification would speed up the electronic procedures that the private sector carries out with the State. Likewise, 85.10% of respondents believed that digital certification would reduce transaction costs
- In conclusion, after having tested the hypotheses and analyzed the tables and graphs elaborated in the questionnaire of the field work, we can affirm that digital certification would allow an efficient administrative management in the state institutions

Keywords: Digital certification, administrative management, state institutions, efficient management, electronic media.

x

INTRODUCCIÓN

Con el objetivo de fortalecer las operaciones empresariales, resulta primordial generar en el usuario de Internet, la confianza necesaria en herramientas informáticas que faciliten las actividades tanto de personas como de empresas, así como ofrecer seguridad jurídica a los operadores económicos, que han tomado parte en estas operaciones y han podido darse cuenta que el futuro de la sociedad está en la Red.

Como es sabido, la firma manuscrita es todavía la forma más utilizada y "confiable" para relacionar un documento con una persona en particular, de manera legal. Sin embargo, este método ha adolecido y sigue adoleciendo de diversas imperfecciones, entre ellas la posibilidad de falsificación y las dificultades en el proceso de verificación de la firma.

La firma en sí, involucra dos acciones: la acción de firmar y la acción de verificación de la firma. La acción de firmar, en el caso de la firma manuscrita, consiste en que una persona deje su rúbrica; mientras que la acción de verificación es más complicada ya que se requiere en algunos casos la utilización de tecnología altamente sofisticada y siempre con probabilidad de error.

Otra limitación que se presenta en las distintas transacciones económicas, como la gestión administrativa de una institución, es la necesidad de contar con la presencia física y simultánea de las personas involucradas y la presencia de un notario que garantice la validez de ésta, lo cual hace lenta y costosa una transacción entre organizaciones ubicadas en diferentes partes de un país o del mundo. Precisamente

como alternativa a estos problemas nace una nueva tecnología que puede reemplazar a la firma manuscrita, y que se ha denominado firma digital.

En ese sentido, debemos encontrar la mejor manera de ejecutar una gestión administrativa eficiente, utilizando para ello el marco de la certificación digital.

Esta investigación pretende demostrar la importancia de aplicar la certificación digital como una moderna herramienta de gestión que permitiría una gestión administrativa eficiente de las instituciones del estado peruano.

Este trabajo de investigación se divide en cinco capítulos. En el primer capítulo se plantean los antecedentes, el planteamiento del problema, los objetivos, justificación, alcances y limitaciones y la definición de variables.

En el segundo capítulo se presenta el marco teórico de la investigación, que incluye; las teorías generales relacionadas con el tema, las bases teóricas especializadas, el marco conceptual que define muchos conceptos utilizados en la presente investigación y las hipótesis de estudio.

En el tercer capítulo se explica el método de la investigación, es decir; el tipo, el diseño, la estrategia de prueba de hipótesis, las variables, la población, la muestra, las técnicas de investigación, los instrumentos de recolección de datos y el procesamiento y análisis de datos.

En el cuarto capítulo se realiza la contrastación de hipótesis y el análisis e interpretación de la prueba de campo.

Finalmente en el capítulo cinco, se discuten los resultados de la cual se derivan las conclusiones y recomendaciones del presente trabajo de investigación.

CAPÍTULO I

PLANTEAMIENTO DEL PROBLEMA

1.1 ANTECEDENTES BIBLIOGRÁFICOS

En el desarrollo de la presente investigación se han estudiado los trabajos más actuales y relevantes que se han realizado sobre el tema. Así, Contreras[1], explica que:

En nuestro tiempo las nuevas tecnologías de Información y comunicación han transformado con su aplicación, casi todas las actividades que el ser humano realiza en el umbral de este siglo XXI. En el presente momento histórico son tecnologías e informaciones que circulan en todas las direcciones, están disponibles en cualquier momento y ya no dependen de limitaciones tales como las horas de servicio de oficina pública o de las posibilidades reales de traslación física.

Ello nos lleva a pensar que el Derecho tiene que seguir innovándose para dar soluciones a los nuevos esquemas cambiantes y no quedarse con las instituciones obsoletas, dejando en claro que los principios esenciales conservan su valor, puesto que la libertad, la justicia y la solidaridad entre sociedad y gobierno tienen más que nunca vigencia. Visto de esta manera, la ciencia del Derecho y específicamente la actividad notarial, se insertan paulatinamente en el moderno esquema de sociedad digital, para dar paso a una nueva generación de actividades y procesos sistematizados, cada vez más lejos del papel, considerado como elemento fundamental en la certificación de documentos de orden legal y que hasta hoy ha sido el sustrato básico del oficio notarial.

La transformación de las relaciones sociales vinculadas a este proceso de globalización influye en la celebración de acuerdos de voluntades y estos generalmente son originados del tráfico mercantil para posteriormente extenderse al ámbito del derecho privado como la fuente primordial de las obligaciones.

[1] Contreras López Irma (2009). La firma electrónica y la función notarial en Jalisco, tesis para optar el grado de maestro en derecho, Universidad de Guadalajara

Entendiendo como contrato pues al instrumento técnico para crear entre las personas (intervinientes) relaciones jurídicas y así regular sus múltiples necesidades personales a las que el ordenamiento jurídico reconoce efectos jurídicos. Por ello, los avances tecnológicos traen consigo cambios en todos los campos sociales ocasionando que las sociedades evolucionen y se produzcan cambios importantes, como lo son; generar nuevos ordenamientos o adecuar las leyes existentes a las nuevas necesidades.

Hay que considerar que en los últimos años el Internet y los medios electrónicos nos han permitido realizar intercambios de información, actos y contratos, con mayor rapidez, debido a que este tipo de intercambio de información a través de mensajes de datos nos ofrece beneficios como ahorro de tinta, papel, almacenamiento y mensajería, además nos evita trasladarnos y porque no considerar que nos ahorra hacer filas.

En ese contexto la firma digital nace de manera justificable desde el momento en que los contratos, las transacciones económicas, las compras o cualquier acto traslativo de dominio entre otras figuras jurídicas de igual importancia, se realizan *on-line*, es decir sin la presencia física de las partes; por ello los mensajes de datos que ostenta una firma electrónica, tiene el mismo efecto que un documento con una firma autógrafa. Su validez dependerá entonces de la fiabilidad de la firma electrónica o mejor aún del método en que esta se generó; así pues el hecho de que una firma sea generada por el usuario a través de medios que mantiene bajo su control (clave privada, contraseña, datos biométricos, tarjeta, chip, etc.), asegurando la imposibilidad de que ocurra una suplantación de personalidad, entonces si lo aplicamos al ámbito del derecho notarial, los actos en los que intervenga el notario de igual forma brindarán la certeza y la seguridad jurídica como si fuera plasmado en papel.

En su investigación, llega a las siguientes conclusiones generales:

1. Debido a las cambiantes condiciones y nuevas plataformas de computación disponibles es vital el desarrollo de documentos y directrices que orienten a los usuarios en el uso adecuado de las tecnologías para aprovechar mejor sus ventajas.

2. El auge de la interconexión entre redes abre nuevos horizontes para la navegación por Internet y con ello surgen nuevas amenazas para los sistemas computarizados,

como son la pérdida de confidencialidad y autenticidad de los documentos electrónicos, pero también abre posibilidades para la celebración de transacciones comerciales mediante una identificación con el uso de la firma electrónica sin necesidad de tener que aportar datos personales sensibles.

3. La Criptografía es una disciplina/tecnología orientada a la solución de los problemas relacionados con la autenticidad y la confidencialidad que provee las herramientas idóneas para la sustentabilidad de la firma electrónica.

4. Los usuarios son quienes deben elegir la conveniencia de una u otra herramienta para la protección de sus documentos electrónicos.

5. La creación de los fedatarios públicos electrónicos nos llevará a tener mayor seguridad en la autenticación de los documentos que circulen a través de las líneas de comunicación.

6. Una única Entidad de Certificación de ámbito internacional es inviable, por tanto deberán existir una o varias redes de autoridades por ejemplo Nacionales o Estatales, pero con la celebración de Convenios Federales y Tratados Internacionales.

Mariño[2], señala que: su tesis es un estudio cuantitativo, transversal, hipotético-deductivo sobre el proceso de implantación de la Norma Técnica NTP-ISO/IEC 17799. Código de buenas prácticas para la gestión de la seguridad de la información en las Entidades del Sistema Nacional de Informática del Perú. Esta investigación, se introduce dentro del marco del desarrollo de la Sociedad de la Información, la Agenda Digital Peruana y el Proyecto de Gobierno Electrónico en el Perú y responde a la siguiente pregunta ¿Cuáles son los factores inhibidores que influyen en el bajo nivel de implementación de la Norma Técnica NTP-ISO/IEC 17799 Código de buenas prácticas para la gestión de la seguridad de la información en las Entidades del Sistema Nacional de Informática? Para este propósito, se recopiló información a través de una encuesta semi estructurada en 16 Organismos Públicos Descentralizados adscritas a la Presidencia del Consejo de Ministros (PCM) del

[2] Mariño Obregón Alipio (2010) factores inhibidores en la implementación de sistemas de gestión de la seguridad de la información basado en la NTP-ISO/IEC 17799 en la administración pública, tesis para optar el grado académico de magíster en dirección y gestión de tecnologías de información, facultad de ingeniería de sistemas e informática, Universidad Nacional Mayor de San Marcos

Gobierno Nacional, que tienen su Sede en la ciudad de Lima. La información recopilada en la encuesta, fue procesada y analizada, que permitió luego identificar factores de orden estratégico y operativo causantes del bajo nivel de implantación de la norma.

En su investigación llega a las siguientes conclusiones;

1. Del resultado de la investigación se tiene que los organismos públicos descentralizados adscritos a la PCM, valoran la importancia de la Norma de Seguridad para la Institución, sin embargo esto no guarda relación con el nivel de implementación alcanzado.
2. Dentro del proceso de implementación Sólo 7 de las 16 Instituciones objeto del estudio han iniciado el proceso de implementación, se evidencia dificultad para establecer un plan documentado para 01 ó 3 años, así como la incorporación de dichos planes en los Planes Operativos Institucionales (POI).
3. En el mismo proceso de implementación, destacamos dos aspectos que resultan clave dentro de las Instituciones objeto de la investigación y que está relacionada con la aplicación de la metodología PDCA (planificación). El 66%, de las Instituciones estudiadas manifiestan dificultades para el establecimiento del documento plan de actividades de 1,2 ó 3 años y su respectiva incorporación dentro del Plan Operativo Institucional (POI), de la revisión de los documentos del Plan Estratégico respectivos y/o objetivos publicados en el portal de transparencia de cada Institución, se evidencia que no existe ninguna mención respecto a la implementación de la Norma como objetivo estratégico ni actividad relacionada.

En tal sentido se confirma, de acuerdo al análisis que la Seguridad de la información no está comprendido dentro del proceso de planificación estratégica que realizan dichas Instituciones y por lo tanto no constituye un objetivo estratégico dentro de las instituciones estudiadas, no hay una plan establecido a nivel estratégico para la seguridad de la Información. En consecuencia no hay metas y objetivos concretos a este nivel que se puedan reflejar con consistencia en el Plan Operativo y Presupuesto Institucional, como además; manda la Ley 28411 Ley General del Sistema Nacional de Presupuesto, el cual señala claramente que el presupuesto Institucional se debe

articular con el Plan Estratégico Institucional y que éste a su vez con el Plan Operativo Institucional (POI), de cada Institución.

4. No hay, un entendimiento claro sobre la responsabilidad global de la seguridad de la información dentro de la Institución, lo cual se refleja en que el nivel de liderazgo para la implementación mayormente descansa en los gerentes o jefes de Área de Informática y sin el compromiso de la alta dirección, con un enfoque de seguridad informática más que a la Seguridad de la Información.

Por las razones expuestas, esta investigación, ha determinado que el bajo nivel alcanzado en la implementación de la Norma de Seguridad en los Organismos Públicos Descentralizados Adscritos a la PCM tiene como causa principal el hecho de que la Seguridad de la Información a pesar de formar parte de los objetivos estratégicos del plan de acción de la Agenda Digital Peruana, objetivo No. 5 desarrollo de Gobierno Electrónico, estrategia 5.1, acción No 6 “Desarrollo de un plan de seguridad de la información para el sector público”, y declarado obligatorio por resolución ministerial de la PCM desde el año 2004, no ha sido incorporado en el planeamiento estratégico de cada una de las Instituciones , no forma parte del conjunto de objetivos estratégicos del mismo y como consecuencia no se garantiza las metas presupuestarias correspondientes, dificultando la ejecución de los planes de corto, mediano y largo plazo del proyecto de implementación de la Norma.

5. Como consecuencia del punto anterior y del análisis de los resultados obtenidos en la investigación del proceso de implementación, ha sido posible identificar y calificar en orden de mayor a menor otros factores derivados que dificultan el proceso de implementación entre ellos en primer lugar, la capacitación y concienciación del capital humano, en segundo lugar la falta de Personal especializado en Seguridad de la información. Otro factor importante es la falta de formalización del Área de Seguridad de la Información dentro de las instituciones, pues al no existir una estructura organizativa oficial con roles definidos las actividades de implementación de la norma pierden prioridad dentro de la Institución.

6. Por otro lado, los encuestados también perciben, que en el proceso de Implementación de la norma en las Instituciones no hay un acompañamiento sistematizado del Organismo Rector (ONGEI) a través de talleres o consultorías especializadas sobre la norma, tampoco un mecanismo de control para supervisar el

desarrollo del mismo y sistematizar las lecciones aprendidas enmarcado en un plan maestro de Seguridad de la Información de las entidades públicas.

7. Los logros obtenidos en el proceso de implementación reflejan una madurez de nivel inicial dentro del grupo de Instituciones investigadas, la cual tiene relación con los principales factores que inhiben el proceso y que se señalan en los puntos anteriores.

Aguilar[3], expone que: La seguridad de la información de cualquier organización pública o privada sufre constantemente ataques informáticos provenientes de terceros, incluso desde los usuarios internos que pretenden alterar o comprometer uno de los recursos más valiosos, la información. Por ello, es muy importante emplear un mecanismo certero y robusto, pero a la vez fácil de implementar que permita asegurar la integridad, autenticidad y confidencialidad los datos que residen dentro de una organización sin que se pueda repudiar o negar su autoría.

La tecnología de la firma digital permite garantizar la integridad de los datos y confiar de su procedencia, ya que si se produce una alteración de la información firmada, la firma digital muestra evidencia fehaciente que ha sido alterada o está corrompida y deja de ser íntegro.

Para dicho fin, la firma digital hace uso de un certificado digital, de confianza, que identifica inequívocamente a su poseedor en un mundo digital así como también de un par de llaves matemáticamente relacionadas. Dichos certificados residen en un contenedor criptográfico, el cual garantiza la seguridad y la correcta manipulación mediante aplicaciones de alto nivel que hacen uso del certificado digital.

En el presente trabajo, se implementará un modelo simplificado de firma digital que se soporta en las tecnologías de la PKI y la invocación por protocolos.

Con la adaptación de estas tecnologías, se podrá realizar la firma digital haciendo uso de aplicaciones web con total independencia del navegador, sistemas operativos, ActiveX o cualquier tecnología JAVA (applets, máquinas virtuales de JAVA), evitando así las configuraciones complicadas y dependencias de terceros.

En su investigación llega a las siguientes conclusiones:

[3]Aguilar Alcarráz Gino Brehan (2016) implementación de un modelo simplificado de firma digital basado en la tecnología PKI y la invocación por protocolos caso de estudio: municipalidad de Miraflores, tesis para optar el título profesional de ingeniero de sistemas, facultad de ingeniería de sistemas e informática, Universidad Nacional Mayor de San Marcos

- La implementación de un componente de firma digital web dentro de la municipalidad ha sido posible considerando la tecnología del 4identity (ver tabla 3.6), algoritmo de firma digital RSA (ver Tabla 4.4), algoritmo de Hash SHA2 (ver Tabla 4.2) y el contenedor criptográfico tipo token iAM (ver Tabla 4.6).
- Se ha podido evitar cualquier tipo de independencia de tecnología Java, ActiveX, navegador web, que dificulta la integración y la accesibilidad a las aplicaciones web, y así se cumple el objetivo secundario #1. [HUN, 2012]
- Se ha podido realizar la integración en cualquier navegador haciendo uso de la invocación por protocolos de una aplicación nativa y el uso de un token criptográfico cumpliendo el objetivo secundario #2 [RUNDGREN, 2015] y #5 [CONGRESO DE LA REPÚBLICA DEL PERÚ, 2001] simultáneamente.
- Los gerentes y subgerentes pueden realizar la firma digital con pleno valor legal haciendo uso de este software acreditado ante INDECOPI [INDECOPI, 2008] y el dispositivo criptográfico tipo token iAM, cumpliendo así el objetivo secundario #3 y #4 simultáneamente.
- Con esta nuevo workflow con firma digital web ya no será necesario demandas todas las hojas que la Municipalidad utiliza para imprimir su información y realizar la firma manuscrita, se cumple así el objetivo secundario #6.
- Los dispositivos criptográficos proporcionan mecanismos de seguridad a nivel hardware y software para el uso adecuado de los certificados digitales que residen en él, y deben cumplir con las certificaciones FIPS 140-2 o Common Criteria. Estos no son excluyentes entre sí y dependen de la región en donde se utilicen. [NIST, 2015]
- La seguridad de la firma digital se concentra en el hash resumen de cada documento a firmar. Puesto que se trata de una operación unidireccional, provee la total garantía de que no existe otro documento que pueda generar el mismo hash a través del mismo algoritmo Hash. [PARAG, 2014].
- La firma digital provee la integridad, autenticidad y el no repudio de cualquier tipo de documento electrónico. [KAUR, 2012]
- El sellado de tiempo es el único mecanismo que puede dar fe y confianza en la fecha y hora en los que unos datos han existido y no han sufrido modificación alguna. [STAPLETON, 2005]

- La verificación de la firma digital es una operación compleja que desencripta el hash encriptado y hace la comparación con el hash obtenido al momento de la verificación, si ambos has son iguales entonces el documento no ha sufrido ninguna modificación y se confía en su integridad y autenticidad [KULKARNI, 2014].
- El middleware es un componente software que permite la interpretación de las instrucciones de un dispositivo criptográfico con una aplicación de alto nivel como la firma digital. [FU, 2011]
- Para la aplicación de este modelo, se consideró los aspectos técnicos mínimos soportados tanto en el lado cliente como en el lado servidor [BIT4ID, 2015].
- La tecnología PKI brinda total seguridad y garantía de que cualquier tipo de información que se encuentre firmada digitalmente sea íntegra y autentica.
- Todo nuevo cambio tecnológico o paradigma involucra un esfuerzo perpetuo para que los usuarios utilicen la tecnología de manera adecuada. Si bien el uso de la firma y los certificados digitales se encuentra respaldado por el Estado Peruano, aún no se hace un uso extensivo u obligatorio, pues es un proceso paulatino y constante hasta que todas las entidades públicas y privadas puedan ofrecer servicios digitales a través de la tecnología PKI.
- La tecnología cumple en este caso el rol de facilitar y optimizar los procesos, pero depende en gran medida del uso adecuado del usuario final.
- La firma digital puede ser modificada a través de algunas herramientas, pero siempre dejará evidencia de cualquier modificación al momento de ser validada, y no se podrá confiar del contenido de la firma.
- Se sugiere una autenticación fuerte (o de doble factor), basada en certificados digitales, para el acceso a la intranet de la Municipalidad de Miraflores.
- Se recomienda el uso de certificados digitales SSL a nivel de servidor esto permite garantizar un canal seguro y cifrado entre el servidor y navegador web.
- Este trabajo podrá ser replicado en cualquier otra institución que disponga de un flujo de trabajo basado en web.

Villanueva[4], en su trabajo de investigación llega a las siguientes conclusiones:

A partir de lo desarrollado, y en diálogo con las hipótesis planteadas, se proponen las siguientes conclusiones.

C1: Se ha identificado un proceso que ocurre por la divergencia entre el sistema normativo de uso de los recursos digitales, especialmente del Derecho de Autor; así como las capacidades represivas estatales encargadas de castigar el uso inadecuado de los sistemas técnicos con fines de consumo irregular; frente a los agenciamientos a disposición de los consumidores en el campo digital. Este proceso ha sido llamado incursión digital. Con él se describe la capacidad de los individuos que cuentan con las condiciones técnicas, sociales e infraestructurales ideales, para poder entrar y salir del ámbito de control institucional con facilidad, incursionando en sus propios términos en la sociedad / estado, y obteniendo lo que le interesa con mayores libertades. Podrán surgir sistemas auto-organizados de individuos interesados en lograr más o menos libertades, pero su impacto dependerá de la profundidad de la incursión, que a su vez estará en función de la ya mencionada debilidad institucional para contenerla, y del grado de irregularidad / ilegalidad de lo que se busca lograr.

El proceso se origina en la existencia de sistemas socio técnicos con capacidades específicas que ofrecen la posibilidad de realizar acciones fuera del control de actores de industrias o mercados distintos a aquellos en los que actúa dicho sistema socio técnico. El sistema socio técnico crea affordances, es decir conexiones diádicas y dinámicas entre los medios técnicos y sus usuarios que indican una oferta de acción que puede identificar y ser usada. El uso de esas affordances crea formas de agenciamiento, es decir de aplicación de la agencia a contextos específicos. En el campo digital, es decir en el espacio en donde las prácticas sociales están influenciadas por lo que se ha llamado el habitus hacker, el resultado es incursión digital, el uso de estos agenciamientos para transgredir la capacidad de acción del Estado Nación con fines personales o grupales.

[4] Villanueva Mansilla Eduardo Enrique (2015) la incursión digital y la política pública: nuevos actores a partir del conflicto del derecho de autor en el campo digital, tesis para optar el grado de doctor en ciencia política y gobierno, escuela de posgrado, Pontificia Universidad Católica del Perú

La incursión digital puede limitarse al ámbito del consumo individual o grupal, o ser usada para otros fines, incluyendo lo político, en sociedades autoritarias o democráticas. Sin embargo, la evidencia apunta a que el grueso de los agenciamientos que la producen se orienta a la satisfacción individual de intereses. En ese sentido, la incursión digital es un proceso y una forma nueva de agencia individual, pero no una forma específica de agencia orientada a la política o al activismo.

C2: La existencia de incursiones digitales en el ámbito político no implica impacto político. La capacidad de crear agrupamientos colectivos facilita el establecimiento de redes alrededor de comunidades de práctica latentes, pero no necesariamente hace más fácil tener efectos en la política, dado que los agrupamientos en sí mismo no tienen agencia. La agencia se logra mediante intervenciones en el sistema político (polity), para lo cual se necesitan formas de asociación más convencionalmente orientadas a la intervención e incidencia. En particular, los agrupamientos transnacionales requieren encontrar mecanismos de conexión con activismos concretos en cada Estado Nación para ganar agencia.

Esto no niega que un agenciamiento propio del activismo digital, y en particular del llamado hacktivismo digitalmente correcto, es la creación de discursos unificadores de las comunidades de práctica. Sin embargo, el éxito en la creación de estos discursos no implica efectividad política.

C3: El conflicto del Derecho de Autor (DA) no tiene una solución normativa a la vista; no parece tener cómo resolverse en términos políticos; y solo la transformación del mercado de contenidos protegidos está creando una resolución al ofrecer alternativas a los consumidores. En particular, la resolución normativa es inviable porque los conflictos creados por el consumo irregular y el hacktivismo del DA nacen de la existencia de facilidades sociotécnicas, en la forma de affordances, aprovechadas por los consumidores; estas affordances orientadas al consumo irregular no son fácilmente controlables mediante los recursos legales o técnicos a disposición de los derechohabientes. Sin embargo, los intereses de los derechohabientes, que han creado el sistema global latente del DA, no muestra posibilidades de adaptación ni al nivel de las normas mismas, ni mucho menos al

nivel de la articulación política de los intereses corporativos con los mecanismos de formulación de normas internacionales.

En otras palabras: el sistema global latente del DA no tiene interés en resolver el problema del consumo irregular ni de facilitar el acceso a las posibilidades que ofrecen la tecnología para mejorar el acceso a la cultura y el conocimiento; mientras que carece de capacidad real de detener la transgresión individual de las normas. Esta disonancia aparece como un resultado directo de un conjunto de incursiones digitales capaces de desestabilizar la industria, y de cuestionar la pertinencia del modelo de gobernanza, pero que no son capaces de forzar un modelo alternativo de gobernanza que reconozca los intereses de los consumidores y la transformación de los mercados gracias a la disponibilidad de tecnología. En todos estos casos, tenemos un discurso que se justifica en una heurística atrapada por atajos cognitivos, que proponen que la protección es positiva porque beneficia a los creadores intelectuales; reforzada por dependencias de camino.

C3.1: en el caso de los EEUU, la dependencia financiera de los representantes electos de los aportes de la industria cultural, causada por la naturaleza poliárquica del sistema político, hace inviable pensar en una alternativa de política pública. La dependencia de camino está marcada por la debilidad del sistema político para alejarse de los intereses que lo financian.

C3.2: en el caso de Francia, los intereses de los conglomerados locales y la búsqueda de sincronía con las acciones pro-globalización de los aliados económicos, hace presa fácil del DA, que termina siendo usado para justificar el alineamiento con los intereses de las transnacionales.

C3.3: el caso de Brasil es distinto hasta cierto punto: por tamaño, singularidad cultural y sobre todo tradición política, no está atado a tratados y acuerdos de la misma manera que otros países, y además quiere destacarse como un camino a seguir, diferente del que necesariamente aceptan los demás países. Sin embargo, son parte del sistema mundo y por ello no pueden escapar por completo de las presiones para el cumplimiento de las normas. Es posible que con la aprobación del Marco Civil para la Internet, Brasil logre desarrollar los rudimentos de una política distinta, pero será necesario esperar para tener más material, antes de llegar a conclusiones.

C3.4: el Perú carece de recursos para hacer cumplir sus obligaciones internacionales en el campo del derecho de autor, y su industria cultural se ha adaptado, sin un plan o claridad sobre los efectos de mediano plazo, a las demandas de la capacidad de incursión digital de los consumidores peruanos. No parece haber incentivo alguno para cambiar las políticas públicas, ni para innovar. Los consumidores con los agenciamientos necesarios seguirán disfrutando del consumo irregular, pero esto podrá ser motivo de aumento de las demandas represivas de origen foráneo, en la medida que el país quiera dinamizar su relación con los mercados externos. Por otro lado, la ausencia de discusión sobre políticas orientadas a mejorar el acceso a contenidos culturales no oculta el hecho que no se cuenta todavía con alternativas de políticas que logren aprovechar el potencial del sistema socio-técnico que llamamos Internet, y del campo digital como espacio de acción.

C4: La Internet es el opio de los consumidores. Crea las condiciones para que no sea necesario discutir o proponer términos de intercambio más favorables a los consumidores en mercados como el de los bienes culturales, y por lo tanto estorba la generación de acción colectiva. Al mismo tiempo, sirve para introducir mecanismos de control potencial y actual que son desconocidos fuera del ámbito del activismo más enterado de los detalles técnicos de la situación. Como las satisfacciones obtenidas a través del acceso al consumo irregular son altas, socialmente relevantes y sobre todo rápidas, los obstáculos a vencer para acceder al consumo se vuelven mucho menos relevantes que lo que se puede obtener al hacerlo. Pero esto ocurre en la dimensión individual de la búsqueda de gratificaciones. Que se haga uso de la tecnología creada por hackers no implica que se comparta las intenciones políticas de los mismos; que se apoye el discurso político de los hackers en determinado momento no quiere decir que se esté buscando transformar la sociedad, sino apenas garantizar que las condiciones de acción deseadas se mantengan.

Esto no niega el potencial para la creatividad intelectual y artística, o para el activismo político, que asociamos a la Internet. Sin embargo es necesario destacar que los patrones de acceso y consumo de bienes culturales que ha creado logran satisfacer demanda a escalas enormes, y por ello en su dimensión de consumidores, las personas terminan contando con tantas opciones y posibilidades efectivas de consumo que resulta irreal pensar en buscar alternativas que privilegien el desarrollo

cultural frente al mero consumo. De la misma manera, las industrias tradicionales logran con un mínimo de esfuerzo desarrollar alternativas comerciales que les permite abarcar mercados cada vez más grandes, aunque algunos sectores específicos puedan estar perdiendo en comparación.

El resultado es que el consumo irregular se establece como la base misma de la comunicación contemporánea. Mientras se busca la democratización de acceso o distribución como política, el ciudadano consumidor opta por solucionar sus demandas individuales a través de los recursos de la tecnología, cosa que obviamente ocurre con mayor libertad en países donde los estados tienen menor capacidad de control territorial; las normas represivas pueden existir pero no necesariamente tener efectividad alguna.

García[5], resalta que: El comercio electrónico, desde sus inicios, se ha ido desarrollando permanentemente, de maneras muy diversas, bajo distintas modalidades y haciendo uso de las diferentes tecnologías vigentes en cada momento. En épocas recientes, desde la aparición de las tecnologías de información, los medios electrónicos han sido utilizados para realizar operaciones comerciales de toda índole, en atención a las necesidades de los agentes involucrados. Es en este contexto que se logra identificar que el comercio electrónico involucra transacciones comerciales en la cuales se procesan y se transfieren datos digitalizados.

El comercio electrónico exige mucho más que el solo hecho de transferir información, requiere que se proporcione a las partes interesadas una seguridad sobre la información transferida y sus efectos, no solo tecnológica, sino también jurídica. Para lograr atender esta necesidad nace la firma digital, que en términos legales es el equivalente a una firma manuscrita y debe cumplir las mismas funciones principales, como son: la autenticación de la identidad del firmante, la integridad de la información, la confidencialidad de los datos y el no repudio de la información.

---

[5] García Rojas Walter Augusto (2008) Implementación de firma digital en una plataforma de comercio electrónico, tesis para optar el título de ingeniero informático, facultad de ciencias e ingeniería, Pontificia Universidad Católica del Perú

En el Perú y el mundo se han adoptado legislaciones orientadas a permitir, contribuir y fomentar el uso de la firma digital con la finalidad de promover el desarrollo del comercio electrónico en el sector empresarial, el cual comúnmente es conocido como comercio Business to Business (B2B).

Dentro de esta línea de pensamiento, en el caso específico de Perú, se encuentran vigentes desde el año 2000 tres leyes que tienen por finalidad incentivar y promover el comercio electrónico dentro y fuera del Perú. Estas leyes permiten otorgar validez y eficacia jurídica a los documentos electrónicos. Además existen leyes sobre firmas y certificados digitales, así como también leyes relativas a los delitos informáticos.

En su investigación se llega a las siguientes conclusiones;

- La obtención de datos de la firma digital incrustada en los documentos PDF se ha aplicado sólo para documentos que se firman con la plataforma en el proceso de registro o modificación de datos en el mismo momento que esto ocurre, descartándose la posibilidad de obtener los datos de un documento ya firmado con cualquier otra herramienta, ya que no existe la certeza de que corresponda con la persona que realiza el registro o modificación de los datos.
- El esquema de firma de contratos incluye que se generen hasta tres copias por cada contrato: un contrato original sin firmas, un contrato con la firma del vendedor y otro con la firma de ambas partes; esto para tener evidencia de cada etapa del proceso para futuros reclamos legales que puedan suscitarse.
- El primero en firmar un contrato será el vendedor ya que legalmente es el que menos arriesga en un proceso de compra.
- El contrato PDF se visualizará sin ninguna firma o cuando contenga las firmas de ambas partes para no generar ningún tipo de desventaja legal para los involucrados comportándose la plataforma como un notario virtual.
- Tanto la incrustación de la firma digital como la del sello de tiempo dentro de los documentos PDF son tecnologías factibles.
- Todo proceso de firma digital y sellado de tiempo son tecnologías que tienen cien por ciento de valor legal en localidades que cuenten con autoridades de certificación autorizadas o que tengan leyes definidas que los avalen; así, los certificados emitidos fuera del Perú tienen valor legal dentro del territorio.

Reyes[6] en su investigación llega a las siguientes conclusiones:

I.- Internet es un medio, no un fin en sí mismo. El comercio no deja de ser comercio aún cuando tenga el calificativo de electrónico.

II.- México cuenta con legislación que reconoce la validez jurídica del contrato electrónico, su posibilidad de exigibilidad judicial, medios probatorios y criterios para su valoración en juicio.

III.- Para que un mensaje de datos en el que se consignen contratos, convenios o compromisos que den nacimiento a derechos y obligaciones, pueda considerarse legalmente válido, es necesario asegurar que la información en él contenida reúna las siguientes características:

INTEGRIDAD:

Entendida en dos vertientes, la primera respecto de la fiabilidad del método para generarla, comunicarla, recibirla o archivarla. Y la segunda como la forma de garantizar que la información en él contenida no fue alterada. Al respecto la Secretaría de Economía elaboró un proyecto de Norma Oficial Mexicana que establecerá los requisitos que deban observarse para la conservación de mensajes de datos, con fundamento en lo dispuesto por el artículo 49 segundo párrafo del Código de Comercio.

ATRIBUCIÓN:

La forma en que podemos garantizar que las partes que se obligan en la relación jurídica son quienes dicen ser y expresan su voluntad libre de vicios. Esta atribución a las personas obligadas en la relación jurídica que se pretende formalizar en un mensaje de datos, no es más que una "FIRMA ELECTRÓNICA".

ACCESIBILIDAD:

Se refiere a que el contenido de un mensaje de datos en el que se consignen contratos, convenios o compromisos que den nacimiento a derechos y obligaciones, pueda estar disponible al usuario (emisor, receptor, juez, auditor, autoridades, etc.) para su ulterior consulta, siempre y cuando reúna las dos características anteriormente anotadas. Para lo cual deberá establecerse en la legislación federal que al efecto deberá emitirse la forma de presentar a "los usuarios" estos mensajes de

[6] Reyes Krafft Alfredo Alejandro (2002) la firma electrónica y las entidades de certificación, tesis para obtener el diploma de doctor en derecho, facultad de derecho, Universidad Panamericana

datos, la cual podría hacerse previa certificación de atribución e integridad por parte del prestador de servicios de certificación.

IV.- Es de hacer notar la falta de técnica legislativa que se hace patente en la redacción del primer párrafo del artículo 49 del Código de Comercio, que señala: "Los comerciantes están obligados a conservar por un plazo mínimo de diez años los originales de aquellas cartas, telegramas, mensajes de datos o cualesquiera otros documentos en que se consignen contratos, convenios o compromisos que den nacimiento a derechos y obligaciones. " , toda vez que el Código Civil Federal en su artículo 1793 establece que "los convenios que producen o transfieren las obligaciones y derechos, toman el nombre de contratos".

V.- Actualmente se está trabajando en algunos proyectos legislativos como son las reformas al Código de Comercio en materia de firmas electrónicas y prestadoras de servicios de certificación, Reformas en materia penal en lo relativo al "crimen electrónico", Protección de datos personales, etc.

VI.- En cuanto a la firma es importante destacar que su función más importante es la de ser el instrumento por medio del cual el firmante expresa su voluntad, es la exteriorización de la declaración de voluntad de una persona. Esta exteriorización de la declaración de voluntad puede hacerse por medios electrónicos, siempre que legalmente se atribuya al firmante, es aquí donde cobra fuerza la función identificativa de la misma, para dar certeza de que es él y no un tercero quien asume la obligación.

VII.- La firma electrónica, como comentamos, podemos clasificarla de la siguiente manera: SIMPLE definida como los datos en forma electrónica consignados en un mensaje de datos, o adjuntados o lógicamente asociados al mismo, que puedan ser utilizados para identificar al firmante en relación con el mensaje de datos (partiendo de la presunción, en materia mercantil, de que el mensaje ha sido enviado usando medios de identificación como claves o contraseñas por ambas partes conocidas, para lo cual se requerirá de un acuerdo previo y firmado en forma autógrafa por las partes) o AVANZADA que podemos conceptuar como la firma electrónica que permite la identificación del firmante y ha sido generada bajo su exclusivo control que vincula exclusivamente al mismo con el mensaje de datos al que se adjunta o se asocia, lo que permite que sea detectable cualquier modificación ulterior de éste

(entendida como proceso electrónico que permite al receptor de un mensaje de datos identificar formalmente a su autor, el cual mantiene bajo su exclusivo control los medios para crear dicha firma, de manera que esté vinculada únicamente a él y a los datos a que se refiere el mensaje, permitiendo detectar cualquier modificación ulterior al contenido del mismo, garantizando así la identidad del titular y que éste no pueda desconocer la autoría del documento.

VIII.- Para lo anterior será necesario que se expida legislación federal relativa a la firma electrónica "avanzada" en la que se regule la actividad de los prestadores de servicios de certificación, a los propios certificados de firmas electrónicas, así como la admisibilidad y forma de presentar como prueba en juicio a los mensajes de datos firmados y se establezcan los requisitos técnicos necesarios.

IX.- Debemos distinguir entre lo que comúnmente se denomina "firma digital" y la "firma electrónica avanzada", ya que la primera es una especie de la segunda, esto es, la firma digital es una firma electrónica avanzada elaborada bajo los estándares de la tecnología PKI. Esto quiere decir que denominarla firma digital nos limitaría a una tecnología de encriptación y violaríamos el principio internacional de Neutralidad Tecnológica.

X.- Por último presentamos un proyecto concreto de reformas al Código de Comercio en materia de firma electrónica y prestadora de servicios de certificación

Viega y Rodríguez[7] nos explican que; La historia del Derecho, está condicionada por las tres revoluciones de la escritura, de la imprenta y de la ordenación electrónica de datos. En las tres revoluciones el Derecho es afectado a través del Lenguaje. En la primera se pasa de la expresión oral a la escrita; en la segunda, de la escritura manual a la impresa y en la tercera de la escritura tipológica, impresa o mecánica al lenguaje tratado electrónicamente.

El fenómeno de la desmaterialización responde a la necesidad de cambio y adaptación que va a implicar para el desarrollo de la telemática a un concepto filosófico –antes que jurídico-. En efecto, es físicamente palpable por nuestros sentidos una gradual e ineludible desmaterialización de la realidad. Se observa con

[7] Viega Rodríguez, María José y Rodríguez Acosta, Beatriz (2005) documento electrónico y firma digital, cuestiones de seguridad en las nuevas formas documentales. Instituto de derecho informático de la facultad de derecho de la Universidad de la República de Uruguay, Montevideo

nostalgia, o satisfacción para algunos, el derrumbe de lo físico (el alto grado de la obsolescencia de lo material, la poca permanencia y duración de los objetos y la pérdida de su individualidad) y de lo ético o valorativo lo cual hace recordar la frase del pensador decimonónico: "todo lo sólido se desvanece en el aire". El fenómeno evolutivo de la desmaterialización al resulta equiparable a una alteración contractual de similar importancia a la que se produjo con la sustitución de la tabla o tablilla de piedra o barro por el papiro y la del pergamino por el papel.

El fenómeno de la desmaterialización, desincorporación o espiritualización se manifiesta fundamentalmente en la despersonalización de las relaciones comerciales, en los medios de pago electrónico, en la transferencia electrónica de fondos, en el documento electrónico, en la desmaterialización de los títulos valores, en el auge del comercio electrónico o desnudez del papel, lo que ha llevado a que se hable de la crisis de la sociedad del papel y se proponga un nuevo modelo social o cultural donde el papel será reemplazado por medios informáticos con soportes digitales y transferencia electrónica.

La obra, consta de 8 capítulos y un apéndice normativo, en el que se incluyen las principales normas vigentes en nuestro ordenamiento positivo. Tras la Introducción (capítulo I), se analizan comparativamente el documento tradicional (capítulo II) y el documento electrónico (capítulo III), pasándose revista al Derecho comparado (capítulo IV) y al Derecho uruguayo en la materia (Capítulo V). Del mismo modo, se estudian luego la firma ológrafa frente a las firmas electrónica y digital (capítulo VI), dedicando especial atención a las Autoridades de Certificación (capítulo VII) y al Notariado en la actual encrucijada tecnológica (capítulo VIII).

El apéndice normativo ofrece la ventaja de reunir un conjunto de disposiciones dispersas y cuyas recopilaciones anteriores son parciales o han quedado desbordadas por el tiempo en que fueron realizadas.

Urbina[8] nos detalla que; En la actualidad, el manejo de documentos electrónicos es una tendencia al alza en Chile. Sin embargo, en la actualidad la mayoría de la documentación con valor legal es manejada en papel, no existiendo un

[8] Urbina Mella Cristian Andrés (2012) certificación para la digitalización de documentos en Chile, tesis, para optar al título de ingeniero civil industrial, facultad de ciencias físicas y matemáticas, departamento de ingeniería industrial, Universidad de Chile

procedimiento que permita certificar copias electrónicas de documentos. Es así que el presente trabajo tuvo como objetivo sentar las bases para definir los estándares y procedimientos necesarios para establecer la digitalización certificada en Chile, permitiendo de esta forma otorgarle valor legal a las copias electrónicas de documentos en papel.

El estudio realizado buscó conocer la actualidad legal e idiosincrática del país, analizándose las legislaciones válidas actualmente relacionadas con la gestión documental. Las legislaciones estudiadas fueron la Ley de Microficha y Micrograbación, la Ley de Documento Electrónico y Firma Digital; y la Ley de Acceso Público a la Información. Además se analizaron los distintos puntos de vista de los agentes involucrados, en donde se encontraron dos puntos de vista muy dispares: por un lado se veía a la digitalización certificada como una forma de eliminar los documentos en papel; por otra parte, se consideraba como la mejor forma de resguardar los documentos originales en papel, utilizando sus copias electrónicas.

Se analizaron los procedimientos utilizados por otros países en la aplicación de la digitalización certificada. Principalmente existen dos criterios, en donde España y el Reino Unido tienen una legislación enfocada en la digitalización certificada de documentos públicos, que deben ser digitalizados y certificados por organismos públicos, y cuyo fin es el acceso a dicha información por los ciudadanos. El segundo criterio, reflejado en la legislación de Estados Unidos y Perú, busca certificar documentos generados por instituciones privadas, permitiendo que empresas técnicamente idóneas realicen la digitalización, bajo la fiscalización de una organización.

Dado el estudio de la realidad Chilena e internacional, se presentaron tres propuestas de procedimientos de digitalización. Se determinó que la Certificación Estatal: documentos públicos y privados, es la que mejor se adapta a la realidad nacional, permitiendo certificar documentos digitalizados privados y públicos, siendo el estado el responsable de certificar la autenticidad y veracidad de las copias electrónicas.

En términos generales las propuestas de implementación buscan alinearse con la legislación actual de los documentos electrónicos, que deben ser certificados por

firma electrónica avanzada, siendo este el método seleccionado de certificación. Además, el presente trabajo analizó todos los puntos críticos que debe contener una futura legislación, definiendo cuales son las consideraciones que se deben realizar para definir un procedimiento de digitalización y certificación.

En su investigación llega a las siguientes conclusiones generales;

Durante la investigación que se realizó para generar el presente documento, se conversó tanto con representantes de entidades privadas como entidades públicas, así como personas que conviven continuamente con el manejo de documentos. Si bien sus puntos de vista respecto a los alcances y objetivos que conlleva la digitalización pueden variar, todos concuerdan en que es una necesidad país, tanto para el respaldo de documentos, como facilitador de trámites o un método para disminuir los costos.

Sobre este punto, cabe destacar que hay dos visiones muy marcadas respecto al manejo de documentos y su digitalización: en primer lugar el sector privado ve como factible la posterior eliminación de los originales en papel, una vez que la digitalización sea certificada como fiel copia del original, y que como copia posea valor legal. Mientras que el sector público, sobre todo los archiveros (encargados de almacenar y manejar los documentos públicos), poseen un fuerte arraigo a los documentos en papel, por lo que ven a la digitalización como un respaldo de mucha utilidad, pero que siempre se podrá contar con el original en papel.

Luego, se analizó la realidad de otros países con respecto a la digitalización certificada de documentos. Por ello, al analizar a España, Estados Unidos, Perú y Reino Unido, cuyas legislaciones permiten la digitalización certificada de documentos bajo distintas condiciones y para diferentes tipos de documentos, se buscó conocer de qué forma se implementaron procedimientos para lograr dicha digitalización certificada.

Por una parte, en España y el Reino Unido, la legislación está enfocada a la digitalización de documentos públicos, por lo que el proceso está a cargo de las entidades públicas y ellas son las encargadas de certificar los documentos: esto tiene una gran relación y facilitaría de gran forma la implementación de la Ley de Trasparencia, la cual no ha logrado aplicarse cabalmente como se pensaba en un comienzo.

El caso contrario son las legislaciones de Estados Unidos y Perú, que están enfocadas en la digitalización certificada de documentos privados, si bien en Estados Unidos solo es aplicable a cheque bancarios, la forma en la que está implementada permitiendo que cualquier operador de banco pueda digitalizar el cheque y crear el "cheque sustituto", es un claro ejemplo de cómo se pueden simplificar y aplicar los procedimientos de digitalización.

El caso de Perú es de gran interés debido a que se logra implementar la digitalización certificada de documentos en todos sus niveles, tanto para documentos privados como públicos. Además para lograr mayor alcance, se fomenta la descentralización del servicio, fomentando la creación de empresas que realicen la digitalización certificada de forma local; sin embargo se debe cuidar de reglamentar este proceso de forma muy estricta para evitar posibles fraudes o blanqueamiento de documentos.

El objetivo final del proyecto no busca definir de forma detallada los estándares y procedimientos, esto se debe a que los procedimientos y estándares establecidos deben permitir adaptarse a distintas culturas organizacionales. Por ello se buscó sentar el marco general y los estándares básicos para poder implementar la digitalización certificada de documentos en Chile.

Para ello se determinaron los factores críticos que se deben considerar en la digitalización de documentos y su posterior almacenamiento en el largo plazo, incluyendo políticas de migración tecnológica. Políticas que no se encuentran actualmente normadas por la legislación chilena, a pesar de existir el documento electrónico.

Pinela[9] explica que; En la actualidad se ha evidenciado varios avances en cuanto a la tecnología, los mismos que se han ido aplicando a diversos sectores económicos. Entre estos avances se identifica la aplicación de las firmas electrónicas, las cuales representan una herramienta especialmente para las empresas que se dedican a la comercialización, tanto de forma electrónica como en el comercio exterior. Al igual

[9] Pinela Requena Edison Roberto (2013) análisis de la necesidad de la firma digital en las exportadoras e importadoras guayaquileñas para la creación de una empresa de certificación, tesis de grado que se presenta como requisito para optar por el título de licenciado en publicidad y mercadotecnia, facultad de comunicación social, Universidad de Guayaquil

como han existido avances tecnológicos que han proporcionado grandes beneficios a la sociedad y a las empresas, también ha existido un incremento en los delitos informáticos, por lo tanto, las firmas electrónicas proporcionan un medio seguro para las empresas que realizan actividades de comercio exterior, considerando que la seguridad es un factor necesario en el desarrollo de tales transacciones comerciales. En el marco teórico se detallan los temas relacionados con el tema del presente trabajo de investigación, lo que servirá para sustentar en base a las definiciones de diferentes autores la realización de este trabajo. En cuanto a la metodología aplicada se considera el desarrollo de un tipo de investigación exploratoria a través del estudio de campo, lo cual le permitirá al autor obtener la información necesaria acerca del problema a investigar para poder diseñar la propuesta. La datos para la investigación se obtuvieron de las empresas importadoras y exportadoras de la ciudad de Guayaquil, posteriormente fueron tabulados y analizados. En base a la información obtenida se pudo establecer los parámetros para el desarrollo de la propuesta en cuanto a la creación de la empresa de certificación en la ciudad de Guayaquil. Finalmente, se incluyen las conclusiones;

- Se pudo determinar los factores que han influido en que las empresas no tengan certificación digital es por falta de conocimiento sobre las ventajas que ofrece esta herramienta tecnológica.
- Se definieron las pautas necesarias para el desarrollo de la propuesta que era la creación de una guía de seguridad para el uso de la Firma Electrónica así como la creación de una empresa de certificación digital.
- El estudio determino que existe una gran cantidad de usuarios que desconoce sobre el uso de esta herramienta tecnológica y que debería de existir incentivos para que sea utilizada por los OCE’S o las demás empresas que realizan comercio electrónico.
- La Firma Electrónica al cumplir funciones que le atribuye la firma manuscrita tiene la misma validez legal y se le reconocen los mismos efectos jurídicos, por lo que también puede ser admitida como prueba en algún caso judicial.
- Las entidades de certificación son consideradas como un tercero confiable lo cual es muy importante porque cuando una persona natural o jurídica quiera

adquirir una Firma Electrónica lo haga en una empresa que le brinde todas las garantías para que se sienta respaldado el cliente.

1.2 PLANTEAMIENTO DEL PROBLEMA

Con la evolución de la sociedad y el desarrollo de la industria, se inicia una nueva era marcada fundamentalmente por la innovación en el campo de la tecnología, dando lugar a nuevas herramientas informáticas que facilitan las actividades tanto de personas como de las sociedades. El crecimiento y mejoramiento de la sociedad de la información, aportó de manera positiva en materia de competitividad, siendo necesario el empleo de estas herramientas tecnológicas para promover las distintas actividades económicas en las cual nos involucramos diariamente.

Con el objetivo de fortalecer estas operaciones empresariales, resulta primordial generar en el usuario de Internet, la confianza necesaria en estas herramientas, así como ofrecer seguridad jurídica a los operadores económicos, que han tomado parte en estas operaciones y han podido darse cuenta que el futuro de la sociedad está en la Red.

Nuestro país no es ajeno a la evolución de la sociedad de la información, gracias al trabajo de la Comisión Multisectorial para el Desarrollo de la Sociedad de la Información, se cuenta con un Plan plasmado en la Agenda Digital Peruana organizada en 06 mesas de trabajo, dentro de los cuales la mesa 5 está referida al Proyecto de Gobierno Electrónico cuyo objetivo invoca: Acercar la administración del Estado y sus procesos a la ciudadanía y a las empresas en general, proveyendo servicios de calidad, accesibles, seguros, transparentes y oportunos, a través del uso intensivo de las TICs (CODESI, 2005 p. 67) . Una de las estrategias para el logro de este objetivo, consiste en desarrollar un plan de seguridad de la información en el sector público CODESI (2005), el plan antes mencionado constituye uno de los componentes fundamentales para coadyuvar a la creación de la infraestructura de Gobierno Electrónico. Consecuentemente, dada la necesidad de consolidar y estandarizar las diferentes iniciativas en el sector, el Gobierno Peruano a través de la Presidencia de Consejo de Ministros (PCM), decretó la obligatoriedad de la implantación de la Norma (NTP-ISO/IEC 17799, 2004) código de buenas prácticas

para la gestión de la seguridad de la información en el sector público a partir del 23 de Julio de 2004 por Resolución Ministerial de la PCM RM N° 224-2004-PCM (2004), encargando la supervisión del cumplimiento de la implementación de la norma a la PCM a través de la Oficina Nacional de Gobierno Electrónico e Informática (ONGEI). (NTP/ISO 17799, 2007).

Dentro del plan del Gobierno electrónico uno de los puntos fundamentales es la implementación de la certificación digital que da pie a la firma digital. Como es sabido, la firma manuscrita es todavía la forma más utilizada y "confiable" para relacionar un documento con una persona en particular, de manera legal. Sin embargo, este método ha adolecido y sigue adoleciendo de diversas imperfecciones, entre ellas la posibilidad de falsificación y las dificultades en el proceso de verificación de la firma.

La firma en sí, involucra dos acciones: la acción de firmar y la acción de verificación de la firma. La acción de firmar, en el caso de la firma manuscrita, consiste en que una persona deje su rúbrica; mientras que la acción de verificación es más complicada ya que se requiere en algunos casos la utilización de tecnología altamente sofisticada y siempre con probabilidad de error.

Otra limitación que se presenta en las distintas transacciones económicas, como la gestión administrativa de una institución, es la necesidad de contar con la presencia física y simultánea de las personas involucradas y la presencia de un notario que garantice la validez de ésta, lo cual hace lenta y costosa una transacción entre organizaciones ubicadas en diferentes partes de un país o del mundo. Precisamente como alternativa a estos problemas nace una nueva tecnología que puede reemplazar a la firma manuscrita, y que se ha denominado firma digital. Esta tecnología va llegando poco a poco a diferentes lugares del mundo, y los gobiernos, conscientes de las claras ventajas de ésta, hacen los esfuerzos necesarios para implantarla en sus naciones, promulgando leyes y promoviendo su uso.

En ese sentido, ¿cómo podemos hacer para lograr una gestión administrativa eficiente en las instituciones del Estado, aplicando la certificación digital? Ante ello surgen una serie de problemas, que planeamos desarrollar a lo largo de la presente investigación.

1.2.1 Problema Principal

- ¿Permite, la implementación de la certificación digital, una gestión administrativa eficiente en las instituciones del estado peruano?

1.2.2 Problemas Secundarios

- ¿Permite la identificación electrónica a través de la certificación digital, una gestión administrativa eficiente en las instituciones del estado peruano?

- ¿Permite la protección de la información a través de la certificación digital, una gestión administrativa eficiente en las instituciones del estado peruano?

- ¿Permite la garantía de la integridad de la información a través de la certificación digital, una gestión administrativa eficiente en las instituciones del estado peruano?

1.3 OBJETIVOS DE LA INVESTIGACIÓN

1.3.1 OBJETIVO GENERAL

- Demostrar que la implementación de la certificación digital, permitiría una gestión administrativa eficiente en las instituciones del estado peruano

1.3.2 OBJETIVOS ESPECÍFICOS

- Establecer si identificarse electrónicamente a través de la certificación digital, permitiría una gestión administrativa eficiente en las instituciones del estado peruano

- Entender si la protección de la información a través de la certificación digital, permitiría una gestión administrativa eficiente en las instituciones del estado peruano

- Determinar si garantizar la integridad de la información a través de la certificación digital, permitiría una gestión administrativa eficiente en las instituciones del estado peruano

1.4 JUSTIFICACIÓN

La realización de la presente investigación se justifica porque busca implementar un mecanismo que permita agilizar la toma de decisiones en las diversas instituciones del estado peruano.

Hoy en día los medios digitales son susceptibles de substitución, modificación, y replicación, a menos que estén explícitamente protegidos con el objetivo de que se pueda confiar en estas comunicaciones. Un claro ejemplo es nuestro País, en el entorno administrativo, las Entidades Estatales no hacen uso de medidas de seguridad como la criptografía o certificados digitales para aseguran el envío de información a través de la red, si bien por qué no lo necesitan o no se dan cuenta de su necesidad, o porque no tienen conocimiento de ello. Todas estas necesidades de seguridad son cada vez más exigentes, optando sin duda por el uso de algún mecanismo de seguridad más avanzado, como es una Infraestructura de Clave Pública PKI. Una PKI está considerada en la actualidad como el mecanismo de seguridad más completo. La Criptografía de Clave Pública permite, entre otras cosas, implementar sistemas de firma digital y el cifrado de datos sin necesidad de compartición de secretos. La firma digital garantiza la Integridad y el cifrado garantiza la Confidencialidad, pero indirectamente la criptografía de clave pública también permite garantizar la Autenticidad del receptor del mensaje cifrado o del emisor del mensaje firmado brindándonos un extra que es el no repudio, donde el emisor no va a poder denegar que él fue quien envió el mensaje. Esto se consigue

con el uso de certificados digitales, donde se asigna una identidad a una clave pública.

La investigación una vez concluida, dará importantes aportes para agilizar las decisiones administrativas en las instituciones del Estado, valiéndose de la nueva herramienta llamada certificación digital

1.5 ALCANCES Y LIMITACIONES

A través de la presente investigación se busca una gestión administrativa eficiente en las distintas instituciones del estado peruano, utilizando para ello la moderna herramienta de la certificación digital. Sin embargo, es preciso manifestar las limitaciones que se presentaron a lo largo de la investigación.

Primero, la poca colaboración presentada por los funcionarios y/o empleados conformantes de la muestra y miembros de las instituciones a encuestar, no ha permitido contar con información oportuna y valiosa para el desarrollo de la tesis.

Segundo, la recolección de la información presentó varios imprevistos que se han solucionado con la participación de especialistas y expertos en temas de certificación digital así como en temas estadísticos.

Tercero, la falta de recursos y tiempo no ha permitido profundizar la investigación como al principio se esperaba. Sin embargo, el apoyo oportuno de diversos funcionarios de la administración pública, encargados de las oficinas de gestión administrativa de las instituciones del estado ha permitido finalizar la investigación.

1.6 DEFINICION DE VARIABLES

Variable Independiente:

Certificación digital

Definición: Documento Digital emitido por una Autoridad de Certificación a solicitud de una Autoridad de Registro que garantiza la veracidad de los datos contenidos referentes a una persona física o jurídica.

Variable Dependiente:

Gestión administrativa

Definición: Conjunto de acciones mediante las cuales el directivo desarrolla sus actividades a través del cumplimiento de las fases del proceso administrativo: Planear, organizar, dirigir, coordinar y controlar.

CAPÍTULO II

MARCO TEORICO

2.1 Teorías generales relacionadas con el tema

La seguridad se ha convertido en uno de los problemas más urgentes para las organizaciones. Sean estas privadas, entidades de gobierno y entidades no gubernamentales. Es un requerimiento esencial para el cumplimiento de su misión en un mundo globalmente interconectado y cada vez más informatizado. Este entorno tecnológico cada vez más dinámico y complejo que soporta los procesos y servicios del negocio, condiciona la dependencia casi absoluta de las organizaciones en la información para su desempeño efectivo en el logro de sus metas y objetivos, convirtiendo a la información en el activo clave más importante para su desarrollo, competitividad y su sobrevivencia. De lo dicho anteriormente se reafirma que la información es un activo clave para las organizaciones y como tal está expuesta a amenazas que ponen en riesgo su valor, que es necesario preservar incorporando para ello los principios del Gobierno de la Seguridad de la Información como parte integral de las estrategias, procesos, personal en el marco de Gobierno de las Tecnologías de Información alineadas al Gobierno Corporativo como responsabilidad de la dirección ejecutiva.

2.1.1 Sistema de Gestión de la Seguridad de la Información (SGSI)

En estos años han aumentado significativamente las violaciones de seguridad informática en todo el mundo (por ejemplo, la diseminación de virus y ataques que han resultado en una violación de la confidencialidad de datos almacenados), con importantes secuelas de costos en muchos casos. En general, ante esta situación la respuesta reside en la elaboración de especificaciones suficientemente robustas para garantizar que pueden contrarrestarse las amenazas a la seguridad en cualquier esfera de la infraestructura de comunicaciones; y con el fin de poder tratar las múltiples facetas que presenta el tema de la seguridad de la información, se han creado con la participación de organismos internacionales, regionales y nacionales marcos de seguridad normalizados y códigos de buenas prácticas que proporcionen una base común que permita implementar los sistemas de gestión de la seguridad de la

información en todas las organizaciones sin importar el tamaño y el sector, dando origen al concepto de la SGSI.

SGSI son las siglas utilizadas para referirse a un Sistema de Gestión de la Seguridad de la Información, una herramienta de gran utilidad y de importante ayuda para la gestión de las organizaciones. El SGSI, ayuda en las empresas a establecer políticas, procedimientos y controles en relación a los objetivos de negocio de la organización, con objeto de mantener siempre el riesgo por debajo del nivel asumible por la propia organización. Para los responsables de la entidad; es una herramienta, alejada de tecnicismos, que les ofrece una visión global sobre el estado de sus sistemas de información, las medidas de seguridad que se están aplicando y los resultados que se están obteniendo de dicha aplicación. Todos estos datos permiten a la dirección una toma de decisiones sobre la estrategia a seguir (INTECO, 2009). En definitiva, con un SGSI, la organización conoce los riesgos a los que está sometida su información y los sistemas que los soporta y los gestiona mediante una sistemática definida, documentada y conocida por todos, que se revisa y mejora constantemente(INTECO, 2009). Como está definido por la ISO 27001 (2005) "SGSI es parte de todo el sistema de gestión corporativa basada en riesgos del negocio, para establecer, implementar, operar, monitorear, revisar, mantener y mejorar la seguridad de la información".

2.1.2 Estándares y Regulaciones para la Seguridad de la Información.

El fenómeno de la globalización como proceso político, económico y social en el mundo ha dado lugar al surgimiento de muchas regulaciones. Desde la directiva de la Unión Europea de protección de datos a Basel II o Sarbanes-Oxley, solo para nombrar unos pocos; las organizaciones obligadas a cumplir con estas regulaciones gubernamentales usualmente implementan marcos de trabajo reconocidos como COBIT o ISO 17799, se describe en la siguiente sección los más importantes.

Directivas Internacionales sobre protección de Datos.

Las siguientes directivas y Marcos de Trabajo han sido transcritos del libro The Business Case for Network Security: Advocacy, Governance, and ROI de los autores Paquet y Saxe (2004),

El derecho a la privacidad de datos personales está muy desarrollado en la comunidad Europea, e introducido en 1981 dentro del consejo Europeo. Estas iniciativas fueron seguidas por muchos países alrededor del mundo. En el Perú se trabaja la ley sobre privacidad de los datos informáticos desde setiembre de 1999.

Ley Sarbanes –Oxley (SOX). Marco regulatorio para Gobierno corporativo, reporte financiero y control interno. La sección 404 de la ley manda, entre otros requerimientos de reporte y auditoría, que las compañías establezcan un sistema de controles internos para asegurar un adecuado reporte financiero (agosto, 2002).

Ley de Responsabilidad y Portabilidad de los Seguros de Salud (HIPAA). El objetivo del HIPAA fue reformar el mercado de los seguros de salud y simplificar los procesos administrativos del sector salud, mientras se robustecía la privacidad y seguridad de la información de los pacientes y las entidades relacionada con la salud (agosto, 1996).

BASEL II Accord. Establecimiento de directivas para la implementación de controles para la gestión de riesgo crediticio y operacional para el sector Bancario entró en vigor en el año 2003/2004.*Gramm Leach Billey Act (GLBA).* También conocido como la ley de modernización del sector financiero de 1999. Incluye directivas para la creación de nuevas regulaciones sobre la privacidad y seguridad de la información de los clientes.

California Individual Privacy Senate Bill (SB 1386). Ley del Senado de California sobre la privacidad individual. Que obliga a cualquier organización dentro del estado a notificar cualquier incidencia relacionada con la revelación de la información privada de los residentes de California.

The Federal Information Security Management Act FISMA. Ley Federal de Estados Unidos aprobada en el 2002, que manda a las agencias gubernamentales realizar una evaluación del estado de seguridad para sus sistemas clasificados y no clasificados y que incluya un análisis de riesgo y seguridad antes de la aprobación del presupuesto.

Food and Drug Administration *(FDA.* Regulación para la Industria farmacéutica, establece un conjunto de controles y procedimientos técnicos para el tratamiento de registros y firmas electrónicas.

Consecuentemente, han surgido también para el cumplimiento de estas normativas un grupo de estándares como:

ISO 17799. Recomendaciones de mejores prácticas sobre la Gestión operativa de la Seguridad de la información.

ISO 27001. Especificación estándar de los principales requerimientos para un sistema de Gestión de la Seguridad de la Información, contra la cual las organizaciones pueden certificar.

COBIT. Objetivos de control para la información y tecnología relacionadas. Conjunto de buenas prácticas para la gerencia de TI, usado a menudo para lograr el cumplimiento de regulaciones de las tecnologías de la información.

ITIL. Marco de trabajo muy popular para la gestión de los servicios de Tecnologías de la información.

COSO. Establece un marco de trabajo integrado y una definición común de controles internos, estándares, y criterios contra el cual las compañías y organizaciones pueden evaluar sus sistemas de control.

NIST 800. Instituto Nacional de estándares y Tecnología de los EE.UU, provee guías para la seguridad de los recursos de información basados en computadora, explicando conceptos importantes, consideración de costos e interrelación de los controles de seguridad.

ISO 13335. *E*s un compendio de 5 documentos que de forma práctica aborda la seguridad de las Tecnologías de la Información y orienta sobre los aspectos de su gestión, describiendo aspectos conceptuales, gestión, planificación, selección de controles y la seguridad de las redes.

La norma ISO 15408. Define los criterios comunes de seguridad que las tecnologías de la información deben respetar. Estos criterios comunes permiten la evaluación de las funciones de seguridad a través de once clases funcionales y exigencias de garantía entre ellos la auditoria, la comunicación, soporte criptográfico etc.

2.1.3 Metodologías de Implementación

El modelo cíclico Plan Do Check Act (PDCA).Según Eloff y Eloff (2003), Los SGSI se definen en sus dos aspectos: proceso y producto. Como producto es un sistema de administración que la organización adopta para establecer y mantener la seguridad de la información, como proceso es un sistema iterativo con realimentación y mejora contínua que sigue el modelo Plan Do Check Act (PDCA). Este es uno los modelos más populares, base para todos los Sistemas de Gestión incluyendo el de la Seguridad de la Información, y se apoya en la necesidad de que la Seguridad de la Información esté en continua evolución; además, dicha evolución esté documentada y justificada. Tiene cuatro fases; Planificar, ejecutar, verificar y actuar.

Planificar. En esta primera fase se realiza un estudio de la situación de la Organización (desde el punto de vista de la seguridad), para estimar las medidas que se van a implantar en función de las necesidades detectadas.

Hay que tener en cuenta que no toda la información de la que dispone la organización tiene el mismo valor, e igualmente, no toda la información está sometida a los mismos riesgos. Por ello un hito importante dentro de esta fase es la realización de un Análisis de Riesgos que ofrezca una valoración de los activos de información y las vulnerabilidades a las que están expuestos. Así mismo se hace necesario una Gestión para dichos riesgos de cara a reducirlos en la medida de lo posible. El resultado de este Análisis y Gestión de Riesgos será establecer una serie de prioridades en las tareas a realizar para minimizar dichos riesgos. Puesto que los riesgos nunca van a desaparecer totalmente, es importante que la Dirección de la Organización asuma un riesgo residual, así como las medidas que se van a implantar para reducir al mínimo posible dicho riesgo residual.

Ejecutar. En esta fase se lleva a cabo la implantación de los controles de seguridad escogidos en la fase anterior. En dicha implantación se instalarán dispositivos físicos (HW, SW), pero también se creará o revisará la documentación necesaria (políticas, procedimientos, instrucciones y registros).

Dentro de esta fase es muy importante dedicar un tiempo a la concienciación y formación del personal de la empresa de cara a que conozcan los controles implantados.

Verificar. Es importante que la Organización disponga de mecanismos que le permitan evaluar la eficacia y éxito de los controles implantados. Es por esto que toman especial importancia los registros (evidencias) que dejan los diferentes controles, así como los indicadores que permiten verificar el correcto funcionamiento del SGSI.

Actuar. En esta fase se llevarán a cabo las labores de mantenimiento del sistema así como las labores de mejora y de corrección si, tras la verificación, se ha detectado algún punto débil. Esta fase se suele llevar en paralelo con la verificación y se actúa al detectarse la deficiencia, no se suele esperar a tener la fase de verificación completada para comenzar con las tareas de mejora y corrección.

2.1.4 Criptografía

Tradicionalmente, el ámbito de la criptología ha sido concebido como el que se ocupa de las técnicas de cifrado o codificado destinadas a alterar las representaciones lingüísticas de ciertos mensajes, con el fin de hacerlos ininteligibles a receptores no autorizados. Estas técnicas se utilizan tanto en el arte como en la ciencia. Por tanto, el único objetivo de la criptografía era conseguir la confidencialidad de los mensajes. Para ello se diseñaba sistemas de cifrado y códigos. En esos tiempos, la única criptografía existente era la llamada criptografía clásica, definida como el arte de escribir con clave secreta o de un modo enigmático.

Su finalidad es poder garantizar el secreto de la información enviada por el emisor hacia un receptor y que este sea el único capaz de poder obtener la información tal cual el emisor la ha enviado, sin sufrir la más mínima alteración en el proceso.

Tipos de criptografía:

Criptografía Simétrica

También llamada criptografía de clave privada o criptografía de una clave, es un método criptográfico en el cual se usa una misma clave para cifrar y descifrar mensajes. Las dos partes que se comunican han de ponerse de acuerdo de antemano sobre la clave a usar.

Una vez que ambas partes tienen acceso a ella, el remitente cifra un mensaje usando la clave, lo envía al destinatario, y este lo descifra con la misma clave. (GARCÍA, 2008)

Uno de los principales inconvenientes con este tipo de sistema no está ligado a su seguridad, sino al intercambio de claves. El canal utilizado para el intercambio debe ser lo suficientemente seguro. Una vez que el remitente y el destinatario hayan intercambiado las claves, pueden usarlas para comunicarse con seguridad. Dado que toda la seguridad se centra en la clave, esta tiene que ser difícil de adivinar. Esto quiere decir que el abanico de claves posibles, es decir, el espacio de posibilidades de claves, debe ser amplio. Algunos algoritmos vigentes a fecha de la presentación de este trabajo son: DES, 3DES, AES y Blowfish.

La robustez de este tipo de cifrado se sustenta en el uso de estas dos técnicas:

Transposición o permutación: Es el intercambio de las posiciones de las letras de un texto en claro siguiendo un cierto patrón. El mensaje cifrado contiene las mismas letras del mensaje pero en posiciones diferentes, lo que impide una fácil lectura.

Sustitución: Consiste en que los caracteres de un mensaje permanezcan en sus posiciones originales, pero sustituidos por otras letras, números o símbolos, siguiendo un patrón definido.

Este método de cifrado no es recomendado al día de hoy, pues a través del criptoanálisis se ha venido realizando estudios de los sistemas criptográficos con el fin de encontrarle debilidades y romper su seguridad sin saber la clave secreta compartida.

Los ataques de fuerza bruta han permitido vulnerar los algoritmos de cifrado simétrico, ya que este ataque define el procedimiento según el cual, haciendo uso de un algoritmo de cifrado conocido y de un par de texto claro -> texto cifrado, se realiza operaciones de cifrado y descifrado, respectivamente, para poder encontrar las posibles combinaciones de clave.

Criptografía Asimétrica

Este tipo de criptografía utiliza un par de claves (clave pública y clave privada) para el envío del mensaje: una para cifrar y otra para descifrar el mensaje. Lo que se cifra en emisión con una clave, se descifra en recepción con la clave pública. (GARCÍA, 2008)

Las claves pública y privada son otorgadas por la autoridad de certificación. Aunque ambas claves son propias de cada persona, la clave privada no se transmite nunca y

se mantiene secreta. La clave pública, por el contrario, se puede y se debe poner a disposición de cualquiera, pues fue creada con esa finalidad. Esto no implica ningún problema de seguridad, dado que es imposible deducir la clave privada a partir de la pública.

Se puede cifrar un mensaje con la clave pública y descifrar con la privada, dando confidencialidad al mensaje, ya que solo podrá ser visto por el usuario con la correspondiente clave privada.

De igual manera, se puede cifrar con la clave privada y descifrar con la pública, de modo que se consigue el no repudio al mensaje y que el firmante sea el autor fidedigno.

La ventaja de este tipo de criptografía es que no se comparte la clave privada y los demás participantes pueden verificar el contenido con la misma clave pública.

El más extendido de los sistemas de clave pública es el RSA, que fue desarrollado por Rivest, Shamir y Adleman, y es conocido como criptosistema RSA. Este algoritmo es reversible; es decir, además de permitir cifrar con la clave pública y descifrar con la privada, permite cifrar con la clave privada y descifrar con la clave pública.

Criptografía Híbrida

Este tipo de criptografía utiliza tanto el cifrado simétrico como el asimétrico. Emplea el cifrado de clave pública para compartir una clave para el cifrado simétrico. El mensaje que se envía en el momento se cifra usando la clave única (cifrado asimétrico) y se envía al destinatario.

Dispositivos criptográficos

Son dispositivos hardware que llevan un chip criptográfico que cumple el estándar ISO/IEC 7816 e ISO/IEC 7810. Estos dispositivos criptográficos pueden ser:

Smart card (tarjeta inteligente)

Es un dispositivo de las dimensiones de una tarjeta bancaria que contiene un procesador criptográfico seguro y cuenta con circuitos integrados que permiten la ejecución de cierta lógica programada. También conocidos como tarjetas

inteligentes, son del tamaño de una tarjeta de crédito convencional (ISO/IEC 7816 ID-1) o de tamaño SIM (ISO/IEC 7816 ID-000). Este chip lleva un micro CPU con el cual permite realizar operaciones criptográficas.

Para poder leer la información que lleva el chip, es necesario contar con un smart card reader (lector de tarjetas inteligentes) y tener instalado el middleware del proveedor del chip, de modo que este sea reconocido por el Sistema Operativo del usuario.

Para poder garantizar el uso adecuado del certificado que reside en el chip, se solicitará el ingreso del PIN; de no ingresarlo correctamente, se irán acabando los intentos. Generalmente, los chips incorporan un mecanismo de bloqueo (3 intentos) por cuestiones de seguridad.

Estos chips deben estar certificados con alguna de estas 2 certificaciones internacionales de seguridad:

- FIPS 140-2
- Common Criteria EAL 4+

Para el Estado Peruano, el Documento Nacional de Identidad Electrónico (DNIe) permite identificar a su poseedor tanto física como digitalmente.

El DNIe contiene un chip criptográfico con certificación Common Criteria EAL5 y sistema operativo que implementa las especificaciones de JavaCard 2.2.2 y Global Platform 2.1.1.

Almacena en su memoria EEPROM datos del ciudadano en formato OACI, certificados digitales y datos biométricos. El chip y el sistema operativo cuentan con la certificación FIPS 140-2 Nivel 3. En la siguiente figura se detalla otros aspectos de seguridad física del DNIe.

Token criptográfico

Es un dispositivo criptográfico más versátil, ya que es un lector de chip criptográficos e incorpora el chip criptográfico, todo en un único dispositivo con conexión USB 2.0 tipo A. Estos tokens deben estar certificados con: FIPS 140-2 y/o CC EAL 4+. Algunos tokens emplean mecanismos o sistemas adicionales, como tamper proof (ante cualquier intento malintencionado, el token dejará evidencia) o tamper resistant (ante cualquier uso malintencionado, el chip se dañará y quedará inservible).

HSM (Hardware Security Module)

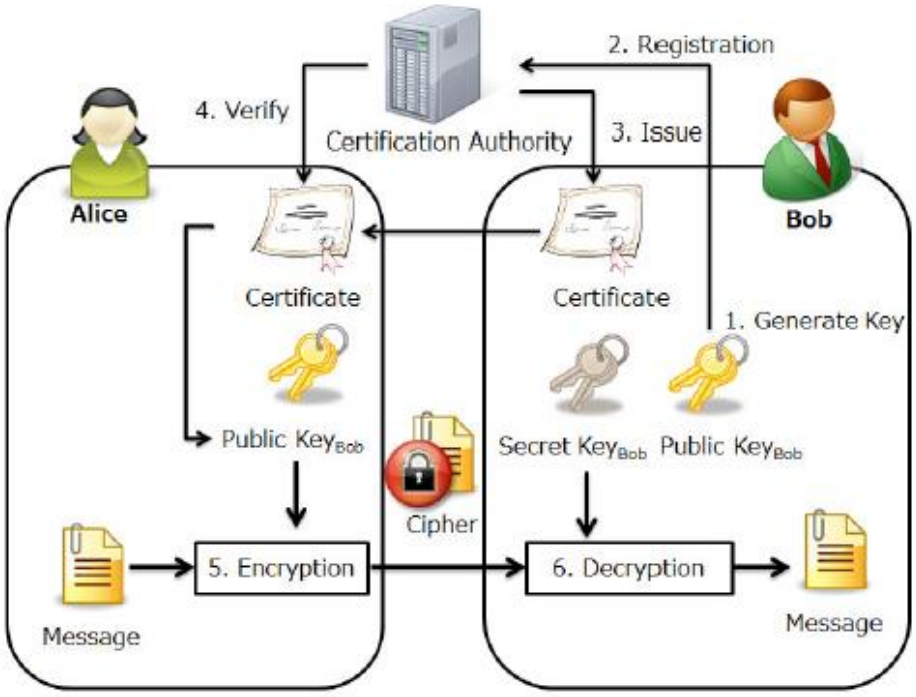
Es un dispositivo criptográfico basado en hardware que genera, almacena y protege claves criptográficas y aporta aceleración hardware para operaciones criptográficas (tps). Estos dispositivos pueden tener conectividad SCSI / IP u otras y aportar funcionalidad criptográfica de clave pública (PKI) de alto rendimiento que se efectúa dentro del propio hardware.

Estandar PKI

Es una combinación de elementos hardware y software, políticas y procedimientos de seguridad que permiten la ejecución con garantías de operaciones criptográficas, como el cifrado, la firma digital o el no repudio de transacciones electrónicas.

Una infraestructura de llaves públicas es un sistema de entrega de certificados y llaves criptográficas, lo cual posibilita la seguridad en transacciones económicas financieras y el intercambio de información sensible entre personas relativamente

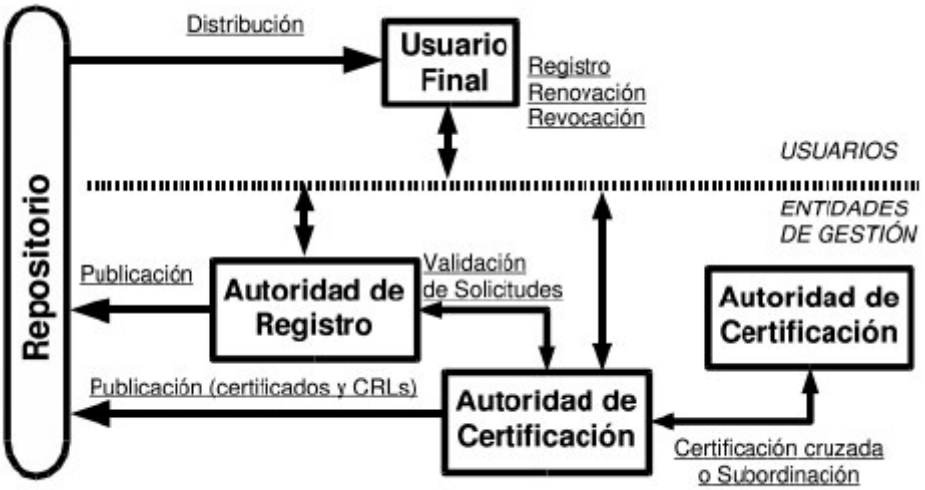
desconocidas (ONGEI, 2002).En la siguiente figura se muestra los procesos básicos de los elementos de un sistema PKI convencional.



En el Perú, la Autoridad Administrativa Competente de la Infraestructura Oficial de Firma Electrónica es INDECOPI (Instituto Nacional de Defensa de la Competencia y de la Propiedad Intelectual). Fundamentalmente, en una Arquitectura de PKI las principales entidades son:

- Una Autoridad de Certificación (CA) que controla el ciclo de vida de los certificados digitales
- Autoridades de Registro (RA) que identifiquen a los usuarios y los cuales se les entrega su respetivo certificado digital
- Suscriptores o usuarios de los certificados
- Repositorios que almacenen los certificados y la lista de certificado revocados (CRL).

En la siguiente figura se visualizan las Autoridades básicas y necesarios que interactúan en un sistema PKI, y adicionalmente el usuario final.



Estándar PKCS

Las Normas de criptografía de clave pública son especificaciones elaboradas por los laboratorios de la RSA en cooperación con los desarrolladores de sistemas seguros en todo el mundo, con el propósito de acelerar el despliegue de la criptografía de clave pública.

Publican por primera vez en 1991 como resultado de reuniones con un pequeño grupo de los primeros en adoptar la tecnología de clave pública, los documentos PKCS han sido ampliamente referenciados e implementados. Asimismo, las contribuciones de las series PKCS se han convertido en parte de muchas de las normas formales. Entre las más importantes contribuciones están los documentos ANSI X9, PKIX, SET, S/MIME y SSL.

A través de los siguientes estándares PKCS, es posible realizar la implementación de firma digital web para la Municipalidad de Miraflores; los demás estándares no serán mencionados, ya que no son requeridos para el presente trabajo.

PKCS #1

Este estándar define el tipo de cifrado RSA. Es un sistema criptográfico de clave pública desarrollado por Rivest, Shamir y Adleman. En honor a ellos se colocó las primeras letras de sus apellidos para darle nombre a este algoritmo. [RSA, 2015].

PKCS #3

Este estándar describe un método para la implementación del acuerdo de claves Diffie-Hellman. La aplicación prevista de este estándar permite el establecimiento de comunicaciones seguras.

PKCS #10

Este estándar se refiere a la solicitud o petición de firma de certificado, o CSR, según sus siglas en inglés. Esta solicitud es enviada a una Autoridad de Certificación para que pueda ser firmada y reconocida dentro de la jerarquía de la clave pública de la AC.

PKCS #11

Este estándar define el API genérico para que se pueda acceder a la información y, sobre todo, al certificado contenido en un dispositivo criptográfico. [RSA, 2015]. Cada proveedor de dispositivo criptográfico provee de las librerías, o middleware, para interactuar. La extensión de estas librerías sigue la extensión de .dll [NCRYPTOKI, 2014]. Cada proveedor de dispositivos criptográficos gestiona un middleware propietario.

PKCS #12

En él se define un formato de archivo con extensión .p12 o .pfx que contiene una clave privada con su respectivo certificado de clave pública, protegiéndolo a través de una clave simétrica.

Dichos archivos pueden ser instalados en un sistema operativo, en sus respectivos contenedores de confianza, tales como:

- Windows: Cryptographic Application Programming Interface (CAPI).
- Linux: Almacén central.
- MAC OX: Llavero.
- Mozilla: Network Security Services (NSS).

Esta práctica no se recomienda, ya que se puede tener tantas identidades digitales como instalaciones de los certificados, sin la posibilidad de tener un control riguroso.

Las buenas prácticas sugieren la custodia de certificados digitales dentro de dispositivos criptográficos (token, smart cards o HSM) que cumplan con las certificaciones internacionales de seguridad.

Esto permitirá asociar una identidad digital a un contenedor seguro y el usuario tendrá un control absoluto del mismo.

2.1.5 Firma y certificación digital

Firma digital

La firma digital es equivalente a la firma manuscrita y permite sustituirla para todos los efectos legales.

La firma digital proporciona seguridad para las transacciones electrónicas haciendo uso de una clave privada y clave pública; también proporciona confidencialidad, autenticidad y el no repudio, a los documentos electrónicos firmados de esta manera. (GAIKWAD, 2015)

Es un valor criptográfico obtenido a partir del resumen digital del certificado y la clave privada de la entidad emisora (CÁNOVAS, 2002).

Una firma digital es un mecanismo criptográfico que permite al destinatario de un mensaje firmado digitalmente determinar la entidad de confianza de dicho mensaje (autenticación de origen y no repudio), y confirmar que el mensaje no ha sido alterado desde que fue firmado.

La firma digital se aplica en aquellas áreas donde es importante poder verificar la autenticidad y la integridad de ciertos datos, por ejemplo, documentos electrónicos o software, ya que proporciona una herramienta para detectar la falsificación y la manipulación del contenido.

Tipos de Firma Digital

Dependiendo de las necesidades del usuario, este puede aplicar los siguientes tipos de firma:

- Firma Simple: Firmas básicas que solo contiene la firma de un único firmante.
- Co-Firma: También conocida por soportar múltiples firmas en un mismo nivel de jerarquía. Para este caso, no importa el orden en el cual se aplica la firma digital; lo importante es que se cuente con todas las firmas requeridas. Se la emplea en documentos de reunión, conferencias, comités, etc.

- Contra Firma: En este caso, el orden de la firma múltiple es importante. Un documento que sigue un flujo normal en el que se necesita que diversos firmantes apliquen su firma, cada uno de estos deberá refrendar la firma del predecesor.

Formatos de firma digital

Según las necesidades y escenarios específicos, se aplica diversos formatos de firmas digitales para los diferentes tipos de archivos.

CAdES (CMS avanzado)

Es el formato binario de firma usado para la encriptación, autenticación, resumen y firma de documentos. Este formato de firma esta soportado en el estándar PKCS#7.

Una vez firmado este archivo, no es posible realizar la verificación y visualización con un programa específico, ya que la información se guarda de forma binaria.

PAdES (PDF avanzado)

Es el formato de uso más frecuente para cualquier aplicación que quiera firmas archivos PDF, ya que un PDF firmado "aparentemente" no sufre ninguna alteración del contenido y para los usuarios es fácil poder realizar las validaciones respectivas.

XAdES (XML avanzado)

Es una especificación desarrollada bajo el amparo del w3c que permite la firma (completa o parcial) de documentos utilizando una notación XML estándar. El formato XAdES ofrece algunas ventajas frente a la firma tradicional, puesto que al estar basado en texto plano, su estructura es legible por humanos.

Funciona de igual manera que el formato CAdES, pero es más extensible y está orientada a documentos XML.

Una firma XML que se utiliza para firmar un recurso fuera del documento XML que la contiene es denominada como una firma separada (detached). Si se utiliza para firmar la firma parcial de un documento que la contiene, es llamada firma envuelta (enveloped). Si contiene los datos firmados dentro de sí mismo, es llamada firma envolvente (enveloping), y en la siguiente figura se aprecia la etiqueta <ds:Signnature ID?> que es donde se contiene la firma digital.

Para los formatos de firma CAdES, PAdES y XAdES, existen variaciones que importa mencionar:

- BES: Es el formato básico para satisfacer los requisitos de la firma electrónica avanzada.
- T: Se añade un sellado de tiempo al documento firmado.
- C: Se añade un conjunto de referencias a los certificados de la cadena de certificación y a su estado de revocación, como base para una verificación longeva.
- X: Se añade sellos de tiempo a las referencias creadas en el paso anterior.
- XL: Se añade los certificados y la información de revocación de los mismos, para su validación a largo plazo.
- A: Permite la adición de sellos de tiempo periódicos para garantizar la integridad de la firma archivada o guardada para futuras verificaciones.

Ventajas de la firma digital

Entre los beneficios más representativos de la firma digital, podemos mencionar los siguientes:

- Permite la integridad de un documento, ya que un archivo firmado digitalmente no puede ser modificado sin dejar un rastro o huella.
- Permite dotar a la firma de una duración de muchos años, así como de una posibilidad de validación en cualquier instante de tiempo.
- Los tiempos de entrega y envío de documentos firmados se reducen considerablemente dentro de una organización.
- Permite garantizar la autoría del documento, evitando así el repudio del documento firmado.
- Permite firmar lotes considerables de documento digitales, los cuales, si fueran llevados al mundo físico, demandarían mucho más tiempo y cansancio.
- La indexación de los documentos firmados es más fácil, puesto que puede ser manipulada por un software de gestión de documentos sin necesidad de complicadas integraciones.
- Garantía legal y respaldo jurídico, ya que la firma digital tiene el mismo valor que una firma manuscrita.

Certificación digital

Autoridad de certificación (CA)

Persona jurídica pública o privada que presta indistintamente servicios de producción, emisión, gestión, cancelación u otros servicios inherentes a la certificación digital. Asimismo, puede asumir las funciones de registro o verificación.

Es la entidad principal del sistema, encargada de tramitar todas las solicitudes relacionadas al ciclo de vida de los certificados. No es posible acceder a ella de manera directa, sino a través de otros elementos intermedios confiables (como el servidor de solicitudes).

Periódicamente, emite certificados digitales asociados a solicitudes pendientes, firma la lista de certificados revocados (CRL) y las políticas de certificación, y publica la información generada en los repositorios de datos tanto internos como externos. (CÁNOVAS, 2002)

Existen jerarquías de CA dentro de una PKI. La CA raíz se firma así misma para garantizar la confianza en ella y luego firma a otras CA subordinadas que confían en la raíz; a esa acción se la conoce como confianza heredada. Los certificados digitales siguen la misma analogía, son firmados por CA subordinadas de confianza.

En una arquitectura PKI, cuando se genera el certificado raíz de una CA, esta queda offline por un periodo determinado de seis meses o un año por cuestiones de seguridad.

Se trata de una autoridad acreditada con la certificación Web Trust para emitir certificados digitales con valor legal, identificando al portador. Es la autoridad a la que el suscriptor solicita una identidad digital o certificado digital (WEBTRUST, 2011).

Autoridad de validación (VA)

Es el ente facultado para suministrar la información sobre la vigencia de los certificados digitales emitidos por las CAs registrados en su RA correspondiente. Realiza esta acción a través de dos protocolos de validación actualmente soportados.

Los protocolos empleados por VA son:

- CRL: Lista de Certificados Revocados.

- OCSP: Protocolo de Estado de Certificados en Línea.

Autoridad de registro (RA)

Normalmente es la primera entidad de contacto con la infraestructura de certificación. Se trata de un software que, gestionado por un operador humano, se encargará de realizar todas las validaciones pertinentes que exija cada operación ejecutada. En líneas generales, la función principal de la RA es la de *identificación* y *validación* de las solicitudes de cualquier tipo. Para realizar sus funciones, toma en consideración las opciones determinadas por la política de certificación del sistema (CÁNOVAS, 2002).

Con excepción de los notarios públicos, es una persona jurídica encargada del levantamiento de datos, comprobación de estos respecto a un solicitante de un mecanismo de firma electrónica o certificación digital, la aceptación y autorización de las solicitudes para la emisión de un mecanismo de firma electrónica o certificados digitales, así como de la aceptación y autorización de las solicitudes de cancelación de mecanismos de firma electrónica o certificados digitales. Las personas encargadas de ejercer la citada función serán supervisadas y reguladas por la normatividad vigente.

La función de las Autoridades de Registro es controlar la generación de certificados para los miembros de una entidad. Previa identificación, la Autoridad de Registro se encarga de realizar la petición del certificado y de guardar los datos pertinentes.

2.1.6 Marco Legal y normativo en el Perú

A continuación, se hace referencia a los documentos que son el aval jurídico para el desarrollo tecnológico de la certificación digital en el Perú:

Ley N° 27269 – Ley de Firmas y Certificados Digitales.

Ley N°27310 – Ley que modifica el artículo 11 de la Ley N°27269.

Ley N°27291 – Ley que permite el uso de medios electrónicos para la manifestación de voluntad y la utilización de la firma electrónica.

Decreto Supremo N°052-2008-PCM – Reglamento de la Ley de Firmas y Certificados Digitales.

Decreto Supremo N° 070-2011-PCM – Decreto Supremo que modifica el Reglamento de la Ley N°27269, Ley de Firmas Certificados Digitales y establece normas aplicables al procedimientos registral en virtud del Decreto Legislativo N°681 y ampliatorias.

2.2 MARCO CONCEPTUAL

Autoridad de Certificación

La Autoridad de Certificación es responsable de brindar las herramientas para poder emitir, con calidad técnica y de manera segura e irrepetible por otros medios o en otras circunstancias, el par de claves, pública y privada, que constituye el eje del certificado

Autoridad de Registro

La Autoridad de Registro es responsable de realizar la identificación de la persona física o jurídica en forma fehaciente y completa, debe efectuar los trámites con fidelidad a la realidad. Además es quien se encarga de solicitar la Aprobación, y/o Revocación de un Certificado Digital. Su objetivo primario es asegurarse de la veracidad de los datos que fueron utilizados para solicitar el Certificado Digital

Certificado Digital

Es un Documento Digital emitido por una Autoridad de Certificación a solicitud de una Autoridad de Registro que garantiza la veracidad de los datos contenidos referentes a una persona física o jurídica.

Cifrado

Para Cifrar un Documento Digital se utiliza la Clave Pública de la persona que recibirá el Documento Digital Cifrado. El proceso de cifrado se hace notablemente más lento cuanto más grande es el Documento Digital que se cifra, o cuanto más grande es la Clave Pública que se utiliza (512 bits, 1024, 2048, etc).

Criptografía

Es la ciencia que se ocupa de la escritura secreta. Si la clave de cifrado es igual a la clave de descifrado hablaremos de Criptografía Simétrica, por el contrario si las claves de cifrado y de descifrado son diferentes hablaremos de Criptografía Asimétrica.

Criptografía Asimétrica

Es aquella que usa para cifrar una clave diferente a la usada para descifrar. Provee métodos que permiten efectuar una comunicación segura entre un Emisor y un Receptor utilizando dos claves diferentes por cada uno, una para cifrar que se llama clave pública y otra para descifrar que es la clave privada. Una clave pública se corresponde con una única clave privada. En la práctica no puede hallarse una clave privada utilizando la clave pública, pues requiere un tiempo de computación absolutamente descomunal aun para los más grandes supercomputadores.

Criptografía Simétrica

Es aquella que usa para cifrar una clave igual a la usada para descifrar. Define un conjunto de métodos que permiten efectuar una comunicación segura entre un Emisor y un Receptor una vez que se ha consensuado una Clave Secreta, con la cual se cifrará el mensaje en el origen y se descifrará en el destino.

Documento Digital

Cuando se habla de Documento Digital se hace referencia a cualquier tipo de información que está almacenada de tal forma que puede usarse o procesarse en computadoras. Algunos ejemplos son: Cartas, Notas, Facturas, Recibos, Comprobantes, Contratos, Legajos, Mensajes, Correo, Fotos, Dibujos, Fax. Voces, Música, Videos.

Eficiencia

Es la capacidad de lograr un efecto deseado, esperado o anhelado con el mínimo de recursos posibles o en el menor tiempo posible.

Entidad Auditante

Es la Entidad que ha sido designada para efectuar la Auditoría y Control de la Autoridad de Certificación.

Estándar PKI

Es una combinación de elementos hardware y software, políticas y procedimientos de seguridad que permiten la ejecución con garantías de operaciones criptográficas, como el cifrado, la firma digital o el no repudio de transacciones electrónicas.

Firma Digital

Para Firmar Digitalmente un Documento Digital se utiliza la Clave Privada del Certificado Digital. El proceso de firma es rápido y puede ser usado con grandes volúmenes de datos sin observarse un decrecimiento importante de la velocidad del computador. Después de firmarse un Documento Digital puede verificarse su integridad usando la Clave Pública correspondiente a la Clave Privada usada para firmar. El proceso de firma consiste en cifrar una cadena de texto llamada digesto, que es confeccionada utilizando funciones que resumen un texto a una cadena de caracteres de longitud fija predeterminada

Gestión administrativa

Conjunto de acciones mediante las cuales el directivo desarrolla sus actividades a través del cumplimiento de las fases del proceso administrativo: Planear, organizar, dirigir, coordinar y controlar

Sistema de gestión de la seguridad de la información (SGSI)

Es un conjunto de políticas de administración de la información. El término es utilizado principalmente por la ISO/IEC 27001, aunque no es la única normativa que utiliza este término o concepto. Un SGSI es para una organización el diseño, implantación, mantenimiento de un conjunto de procesos para gestionar eficientemente la accesibilidad de la información, buscando asegurar la confidencialidad, integridad y disponibilidad de los activos de información minimizando a la vez los riesgos de seguridad de la información.

Órgano Licenciante

Es el organismo del Estado que habilita a una Empresa de Certificación Digital como Autoridad de Certificación.

2.3 HIPÓTESIS

2.3 1 Hipótesis Central:

La implementación de la certificación digital, permitiría una gestión administrativa eficiente en las instituciones del estado peruano

2.3.2 Hipótesis Secundarias:

- Identificarse electrónicamente a través de la certificación digital, permitiría una gestión administrativa eficiente en las instituciones del estado peruano

- La protección de la información a través de la certificación digital, permitiría una gestión administrativa eficiente en las instituciones del estado peruano

- Garantizar la integridad de la información a través de la certificación digital, permitiría una gestión administrativa eficiente en las instituciones del estado peruano

CAPITULO III

METODO

3.1 TIPO

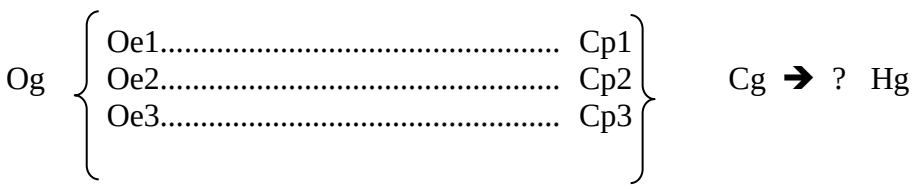
Diversos autores de la metodología de la investigación clasifican los tipos de investigación en cuatro: exploratorios, descriptivos, correlaciónales y explicativos. Asimismo nos señalan que es posible que una investigación se inicie como exploratoria o descriptiva y después llegue a ser correlacional y aún explicativa. El diseño de la presente investigación de acuerdo a las características de las hipótesis formuladas y los objetivos propios de la investigación ha sido enmarcado dentro del tipo de: **investigación explicativa**

También, de acuerdo a la naturaleza del estudio de la investigación, reúne por su nivel las características de un estudio descriptivo, explicativo y correlacionado.

Asimismo, en la presente investigación se utilizaron los métodos; analítico, inductivo, deductivo y descriptivo entre otros, conforme se ha ido avanzando en el desarrollo del trabajo.

3.2 DISEÑO DE LA INVESTIGACIÓN

Para contrastar las hipótesis con la realidad hemos aplicado el diseño no experimental, transeccional y descriptivo utilizando el siguiente esquema:



Dónde:

Og: Objetivo general Oe: Objetivo específico

Cp: Conclusión parcial Cg: Conclusión general

Hg: Hipótesis general

Frente al objetivo general de la investigación se formuló los objetivos específicos de los cuales se obtuvo una conclusión parcial de cada una de ellas, lo que nos llevo a formular una conclusión general que se compara con la hipótesis general planteada

3.3 OPERACIONALIZACION DE LAS VARIABLES

La identificación y tratamiento de las variables que definen las hipótesis, permitirán operativizar y efectuar el proceso de verificación: aceptación o rechazo de los mismos.

VARIABLES	INDICADORES	ESCALA	RELACIÓN
VARIABLE INDEPENDIENTE X. Certificación digital	X.1. Reportes sobre implementación de la certificación digital.	Alta, Media, Baja	X- Y- Z X.1., Y.1., Z X.2. , Y.2., Z X.3., Y.3., Z
	X.2. Cronograma de ejecución de la certificación digital.	Alto, Medio, Bajo	
	X.3. Ratios de avances de la certificación digital.	Alta, Media, Baja	
VARIABLE DEPENDIENTE Y. Gestión administrativa	Y.1. Reportes de gestión administrativa.	Alta, Media, Baja	
	Y.2. Ratios de atención a los usuarios de la institución.	Alta, Media, Baja	
	Y.3. Indicadores de atención de reclamos.	Alta, Media, Baja	
DIMENCION ESPACIAL Z. Instituciones del estado peruano			

3.4 POBLACIÓN

La población objeto de investigación está conformada por el total de la población de 12 instituciones del estado, donde se viene implementado la certificación digital, es decir, 28,566[10] personas.

3.5 MUESTRA

La técnica de muestreo que se utilizará será el ***muestreo probabilístico aleatorio sin remplazo.***

Así, para determinar el tamaño apropiado de la muestra aleatoria se ha considerado aplicar las técnicas probabilísticas teniendo en cuenta la siguiente fórmula:

$$n = \frac{p\,(1-p)}{(e/Z)^2 + [\,p\,(1-p)/P\,]}$$

Donde:

n = tamaño de la muestra
p = probabilidad de éxito (0.88)
e = error esperado 0.05
Z= Valor de la abscisa para una probabilidad del 95% de confianza. Z =.96
P= Población (28,566)

$$n = \frac{0.88\,(1-0.88)}{(0.05/1.96)^2 + [\,0.88\,(1-0.88)/28{,}566\,]} = 161$$

[10] Memorias de las respectivas instituciones del país

Estas 161 personas, conformantes de la muestra, se obtendrán de las 10 instituciones del estado.

3.6 TÉCNICAS DE INVESTIGACIÓN

a) **Técnicas de muestreo**: las técnicas que se usaran para desarrollar esta investigación se centran en la elaboración de una guía para realizar las observaciones en las distintas instituciones del estado con la cual se van a trabajar que nos permitirá verificar la situación técnica administrativa de dichas instituciones, así como una entrevista a expertos y finalmente una encuesta para conocer la opinión de los distintos integrantes de las instituciones con la cual se trabajaran.

b) **Técnicas de procesamiento y análisis de datos**: Se empleó el paquete estadístico Excel para la tabulación que se presenta en frecuencias simples y relativas para el análisis respectivo, así como también el software SPSS. Finalmente se utilizara la prueba de contrastación de hipótesis empleando la distribución del Chi cuadrado con un nivel de un 95% de confianza y un nivel de riesgo del 5%

3.7 INSTRUMENTOS DE RECOLECCIÓN DE DATOS

Se emplearan los siguientes instrumentos:

- ✓ Guía para investigación y recopilación de la información bibliográfica
- ✓ Guía de observaciones

- ✓ Guía de entrevistas a expertos

- ✓ Cuestionarios a los responsables de las instituciones colaboradoras

3.8 PROCESAMIENTO Y ANÁLISIS DE DATOS:

Se empleara el paquete estadístico Excel para la tabulación que se presenta en frecuencias simples y relativas para el análisis respectivo, así como el software SPSS. Finalmente se utilizara la prueba de contrastación de hipótesis empleando la correlación de Pearson con un nivel de un 95% de confianza y un nivel de riesgo del 5%

CAPITULO IV

PRESENTACION DE RESULTADOS

4.1 ANALISIS E INTERPRETACIÓN

A la pregunta:

1. ¿Usted realiza transacciones electrónicas?

Se obtuvo el siguiente resultado:

Tabla No 01

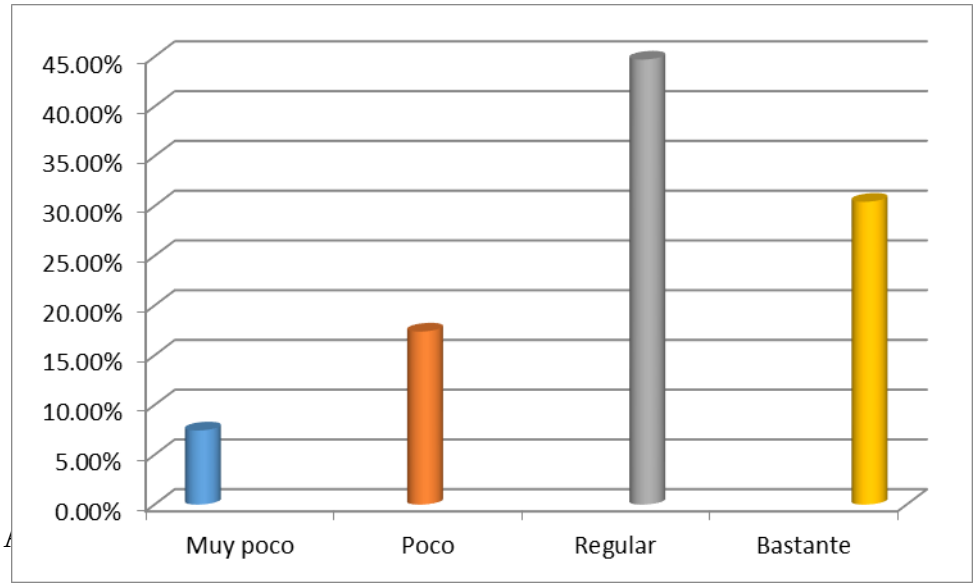
Alternativa	Muestra	%
Muy poco	12	7.45
Poco	28	17.39
Regular	72	44.72
Bastante	49	30.43
Total	161	100.00

Fuente: Encuesta realizada entre el 1 y 12 de mayo del 2017

INTERPRETACION

El 75.15% de los encuestados considera que bastante y regularmente realizan transacciones electrónicas. Asimismo, el 24.85% considera que poco o muy poco.

Gráfico N° 01



la pregunta:

2. ¿Cuantas horas semanales ocupa su tiempo en transacciones electrónicas?

Se obtuvo el siguiente resultado:

Tabla Nº 02

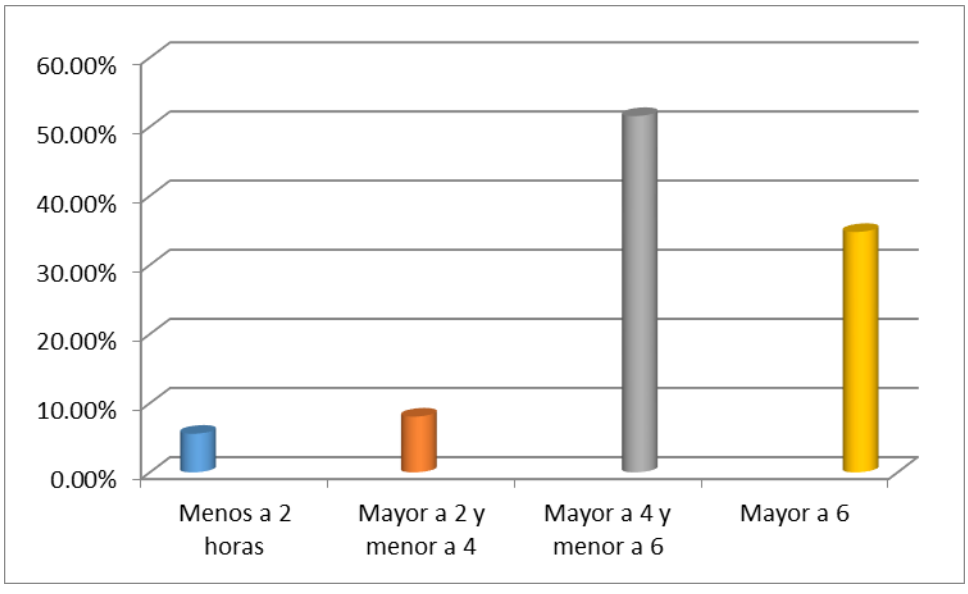
Alternativa	Muestra	%
Menos a 2 horas	9	5.59
Mayor a 2 y menor a 4	13	8.07
Mayor a 4 y menor a 6	83	51.55
Mayor a 6	56	34.78
Total	161	100.00

Fuente: Encuesta realizada entre el 1 y 12 de mayo del 2017

INTERPRETACION

El 51.55% de los encuestados ocupa su tiempo en transacciones electrónicas entre 4 y 6 horas. El 34.78% mayor a 6 horas. El 8.07%, mayor a 2 y menor a 4 y un 5.59% menos a 2 horas.

Gráfico Nº 02



A la pregunta:

3. ¿Entiende las diferencias entre certificado digital y firma digital?

Se obtuvo el siguiente resultado:

Tabla Nº 03

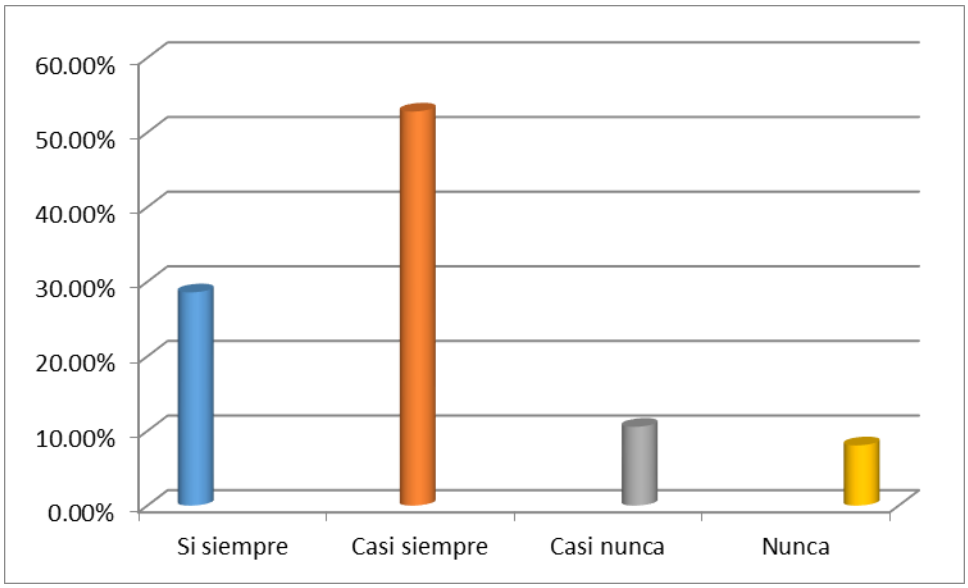
Alternativa	Muestra	%
Si siempre	46	28.57
Casi siempre	85	52.80
Casi nunca	17	10.56
Nunca	13	8.07
Total	161	100.00

Fuente: Encuesta realizada entre el 1 y 12 de mayo del 2017

INTERPRETACION

El 81.37% de los encuestados considera que siempre o casi siempre comprende la diferencia. El 18.63%, considera que nunca o casi nunca lo comprende.

Gráfico Nº 03



A la pregunta:

4. ¿Considera que la certificación digital es un requisito indispensable para que las instituciones ofrezcan un servicio seguro a través de internet?

Se obtuvo el siguiente resultado:

Tabla Nº 04

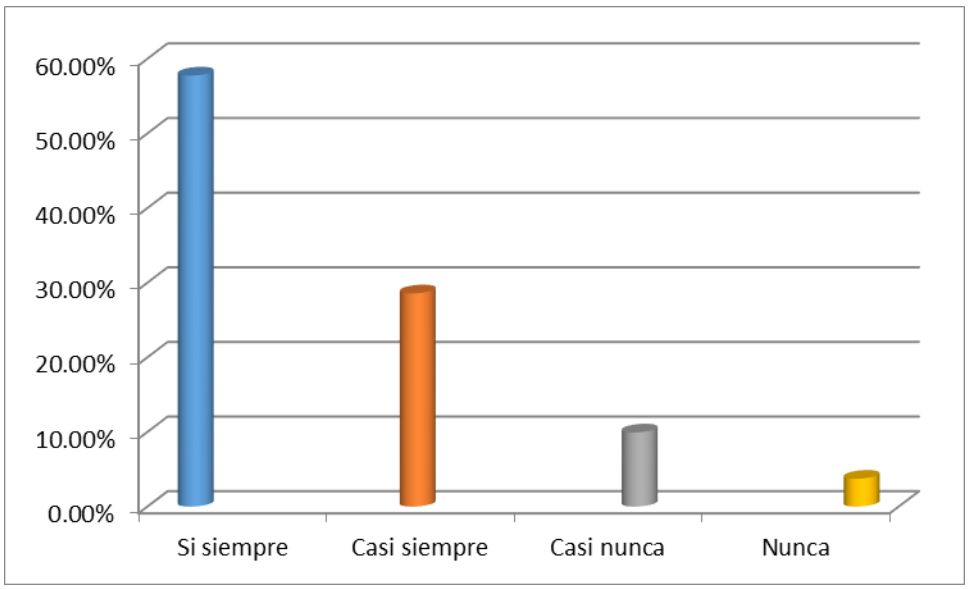
Alternativa	Muestra	%
Si siempre	93	57.76
Casi siempre	46	28.57
Casi nunca	16	9.94
Nunca	6	3.73
Total	161	100.00

Fuente: Encuesta realizada entre el 1 y 12 de mayo del 2017

INTERPRETACION

El 86.33% de los encuestados considera que siempre o casi siempre es un requisito indispensable. El 13.67% considera que nunca o casi nunca es un requisito indispensable.

Gráfico Nº 04



A la pregunta:

5. ¿Conoce las ventajas de la certificación digital?

Se obtuvo el siguiente resultado:

Tabla Nº 05

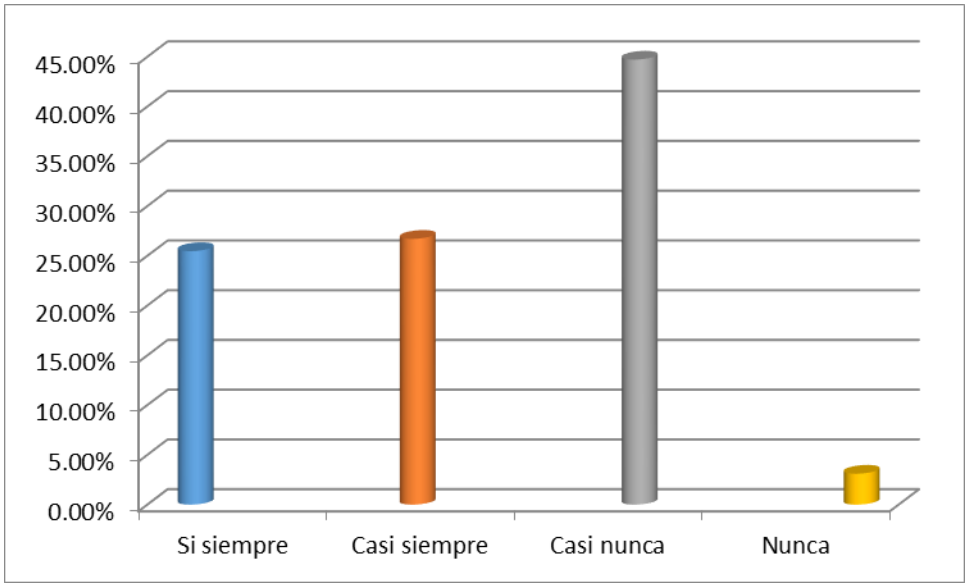
Alternativa	Muestra	%
Si siempre	41	25.47
Casi siempre	43	26.71
Casi nunca	72	44.72
Nunca	5	3.11
Total	161	100.00

Fuente: Encuesta realizada entre el 1 y 12 de mayo del 2017

INTERPRETACION

El 52.18% de los encuestados indica que siempre o casi siempre, conoce las ventajas de la certificación digital. El 47.82% considera que, casi nunca o nunca las conoce.

Gráfico Nº 05



A la pregunta:

6. ¿Identificarse electrónicamente a través de la certificación digital, permitiría una gestión administrativa eficiente en las instituciones del estado peruano?

Se obtuvo el siguiente resultado:

Tabla Nº 06

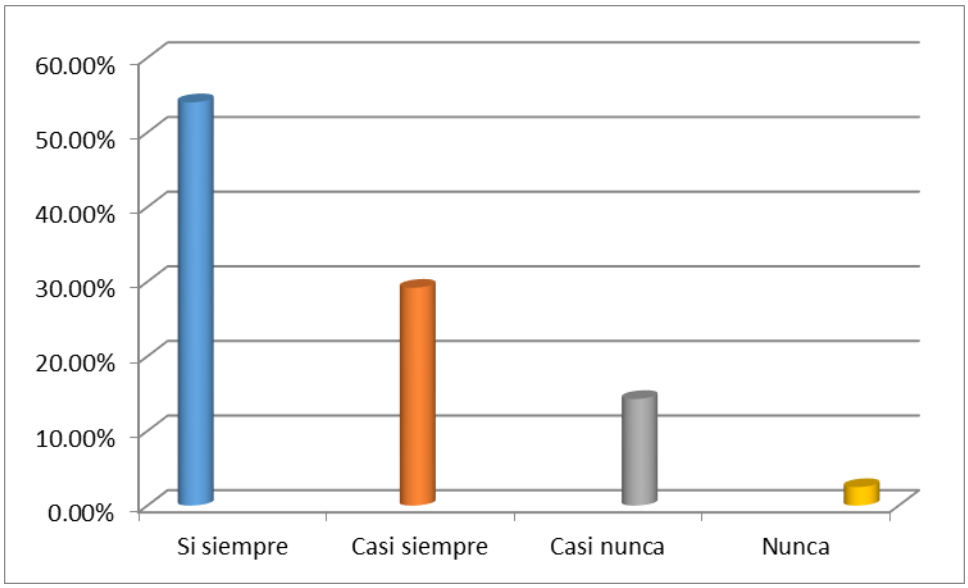
Alternativa	Muestra	%
Si siempre	87	54.04
Casi siempre	47	29.19
Casi nunca	23	14.29
Nunca	4	2.48
Total	161	100.00

Fuente: Encuesta realizada entre el 1 y 12 de mayo del 2017

INTERPRETACION

El 83.23% de los encuestados considera que siempre o casi siempre la certificación digital, permitiría una gestión administrativa eficiente. El 16.77%, considera que nunca o casi nunca lo permitiría.

Gráfico Nº 06



A la pregunta:

7. ¿Considera que los mecanismos de protección de la certificación digital son seguros?

   Se obtuvo el siguiente resultado:

Tabla Nº 07

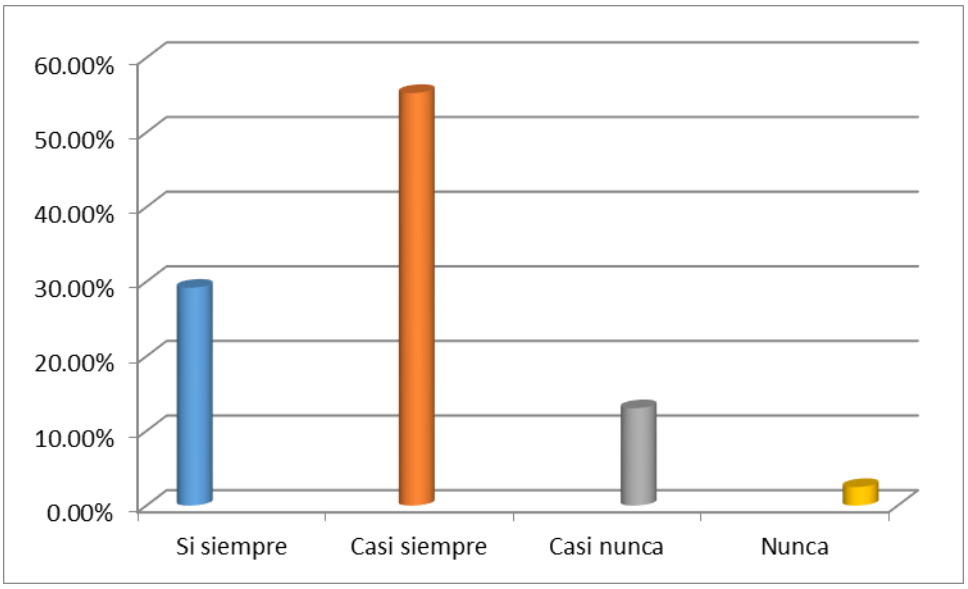
Alternativa	Muestra	%
Si siempre	47	29.19
Casi siempre	89	55.28
Casi nunca	21	13.04
Nunca	4	2.48
Total	161	100.00

Fuente: Encuesta realizada entre el 1 y 12 de mayo del 2017

INTERPRETACION

El 84.47% de los encuestados manifiesta que siempre o casi siempre los mecanismos de protección de la certificación digital son seguros. El 15.53%, considera que nunca o casi nunca son seguros.

Gráfico Nº 07



A la pregunta:

8. ¿Cree usted que la seguridad de los mecanismos de protección de la información a través de la certificación digital lograría incrementar las transacciones electrónicas?

   Se obtuvo el siguiente resultado:

Tabla Nº 08

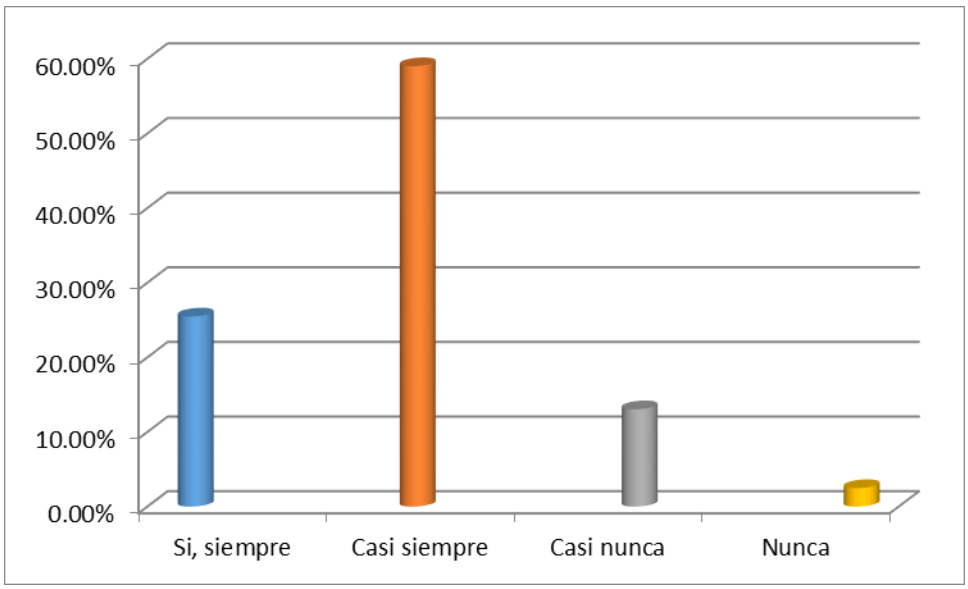
Alternativa	Muestra	%
Si siempre	41	25.47
Casi siempre	95	59.01
Casi nunca	21	13.04
Nunca	4	2.48
Total	161	100.00

Fuente: Encuesta realizada entre el 1 y 12 de mayo del 2017

INTERPRETACION

El 84.48% de los encuestados manifiesta que siempre y casi siempre incrementarían las transacciones electrónicas. El 15.52% considera que nunca y casi nunca lo incrementaría.

Gráfico Nº 08



A la pregunta:

9. ¿Difundir los mecanismos de protección de la información permitiría que más usuarios utilicen la certificación digital?

   Se obtuvo el siguiente resultado:

Tabla Nº 09

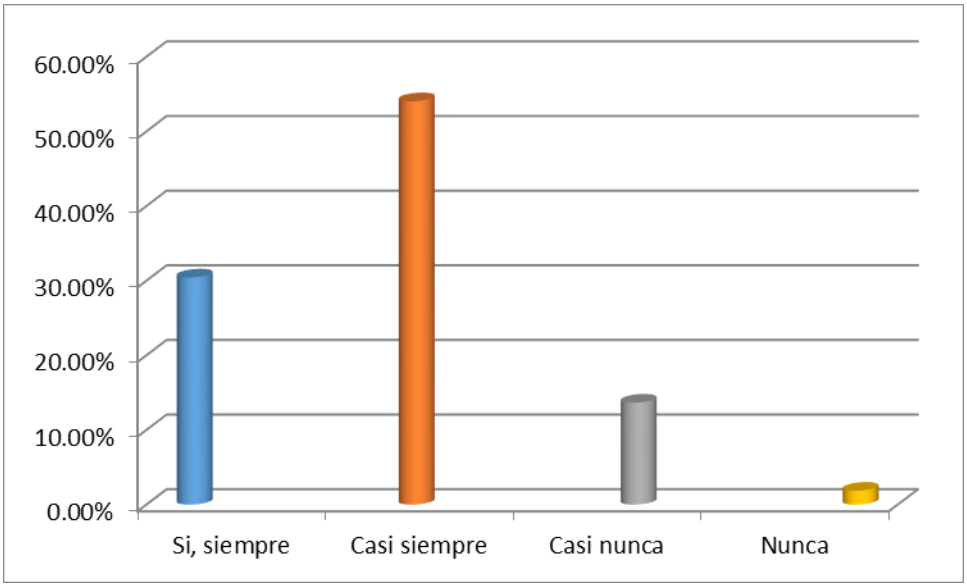
Alternativa	Muestra	%
Si siempre	49	30.43
Casi siempre	87	54.04
Casi nunca	22	13.66
Nunca	3	1.86
Total	161	100.00

Fuente: Encuesta realizada entre el 1 y 12 de mayo del 2017

INTERPRETACION

El 84.47% de los encuestados manifiesta que siempre o casi siempre difundir los mecanismos permitiría que más usuarios utilicen la certificación digital. El 15.53% dice que nunca o casi nunca lo permitiría.

Gráfico Nº 09



A la pregunta:

10. ¿La protección de la información a través de la certificación digital, permitiría una gestión administrativa eficiente en las instituciones del estado peruano?

Se obtuvo el siguiente resultado:

Tabla Nº 10

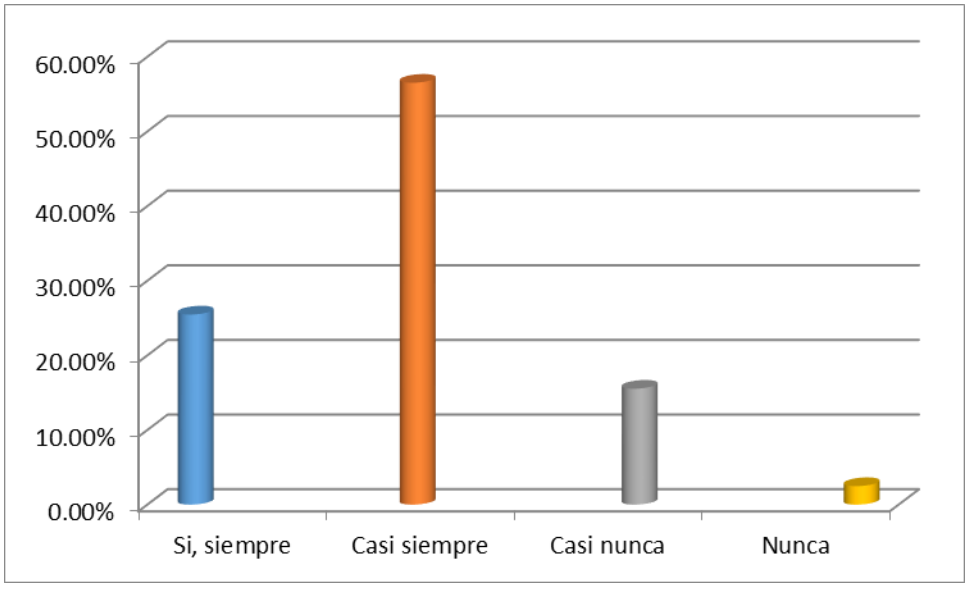
Alternativa	Muestra	%
Si, siempre	41	25.47
Casi siempre	91	56.52
Casi nunca	25	15.53
Nunca	4	2.48
Total	161	100.00

Fuente: Encuesta realizada entre el 1 y 12 de mayo del 2017

INTERPRETACION

El 81.99% de los encuestados considera que sí, siempre o casi siempre la protección de la información, permitiría una gestión administrativa eficiente. El 18.01%, considera que nunca o casi nunca lo permitiría.

Gráfico Nº 10



A la pregunta:

11. ¿Considera que la información a través de la certificación digital puede ser vulnerada?

    Se obtuvo el siguiente resultado:

Tabla Nº 11

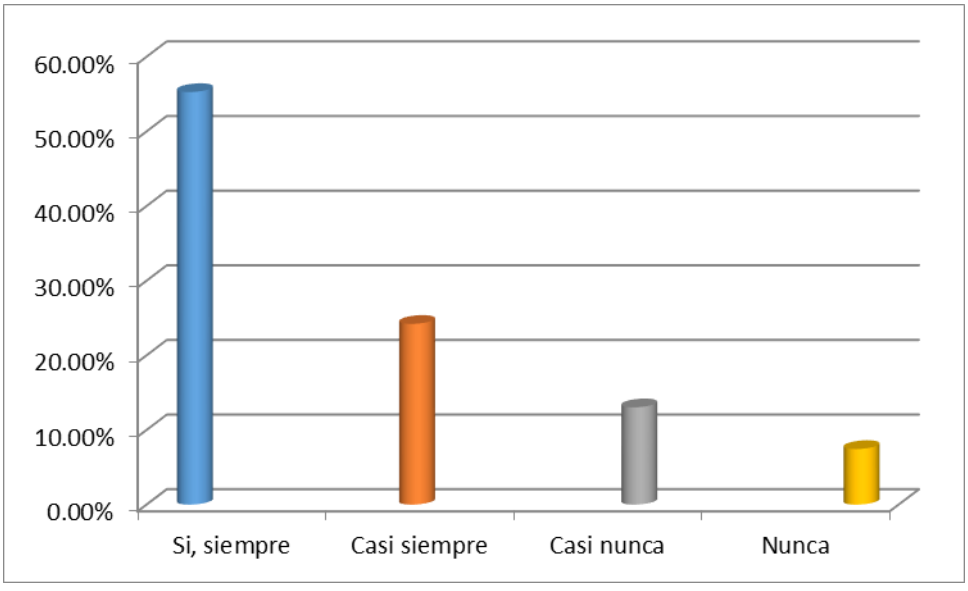
Alternativa	Muestra	%
Si, siempre	89	55.28
Casi siempre	39	24.22
Casi nunca	21	13.04
Nunca	12	7.45
Total	161	100.00

Fuente: Encuesta realizada entre el 1 y 12 de mayo del 2017

INTERPRETACION

El 79.50% de los encuestados manifiesta que siempre y casi siempre la certificación digital puede ser vulnerada. El 20.50%, considera que nunca o casi nunca podría ser vulnerada.

Gráfico Nº 11



A la pregunta:

12. ¿La integridad de la información a través de la certificación digital evitaría la falsificación de la información digital de las personas?

    Se obtuvo el siguiente resultado:

Tabla Nº 12

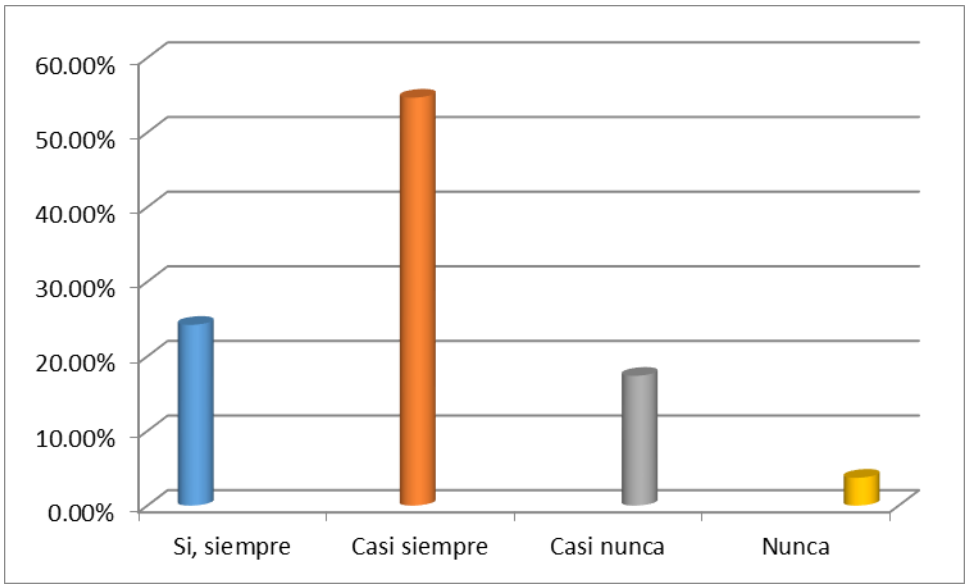
Alternativa	Muestra	%
Si, siempre	39	24.22
Casi siempre	88	54.66
Casi nunca	28	17.39
Nunca	6	3.73
Total	161	100.00

Fuente: Encuesta realizada entre el 1 y 12 de mayo del 2017

INTERPRETACION

El 78.88 de los encuestados manifiesta que siempre o casi siempre la certificación digital evitaría la falsificación de la información. El 21.12%, considera que nunca o casi nunca lo evitaría.

Gráfico Nº 12



A la pregunta:

13. ¿Garantizar la integridad de la información a través de la certificación digital, permitiría una gestión administrativa eficiente en las instituciones del estado peruano?

    Se obtuvo el siguiente resultado:

Tabla Nº 13

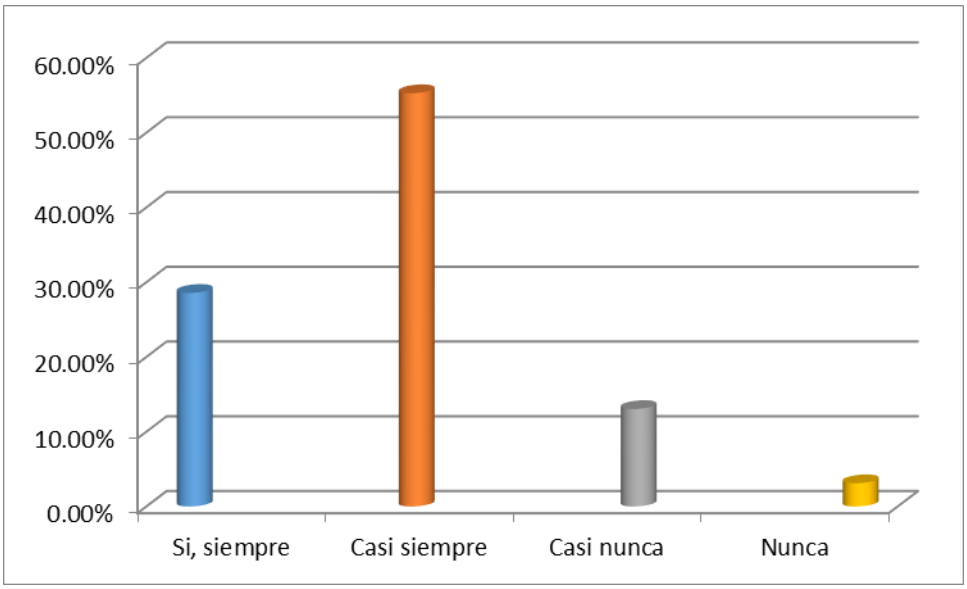
Alternativa	Muestra	%
Si, siempre	46	28.57
Casi siempre	89	55.28
Casi nunca	21	13.04
Nunca	5	3.11
Total	161	100.00

Fuente: Encuesta realizada entre el 1 y 12 de mayo del 2017

INTERPRETACION

El 83.85% de los encuestados considera que siempre y casi siempre garantizar la integridad de la información permitiría una gestión administrativa eficiente. El 16.15% considera que nunca o casi nunca lo permitiría.

Gráfico Nº 13



A la pregunta:

14. ¿Considera usted que la certificación digital ayudaría a reducir la burocracia en las instituciones del estado?

Se obtuvo el siguiente resultado:

Tabla Nº 14

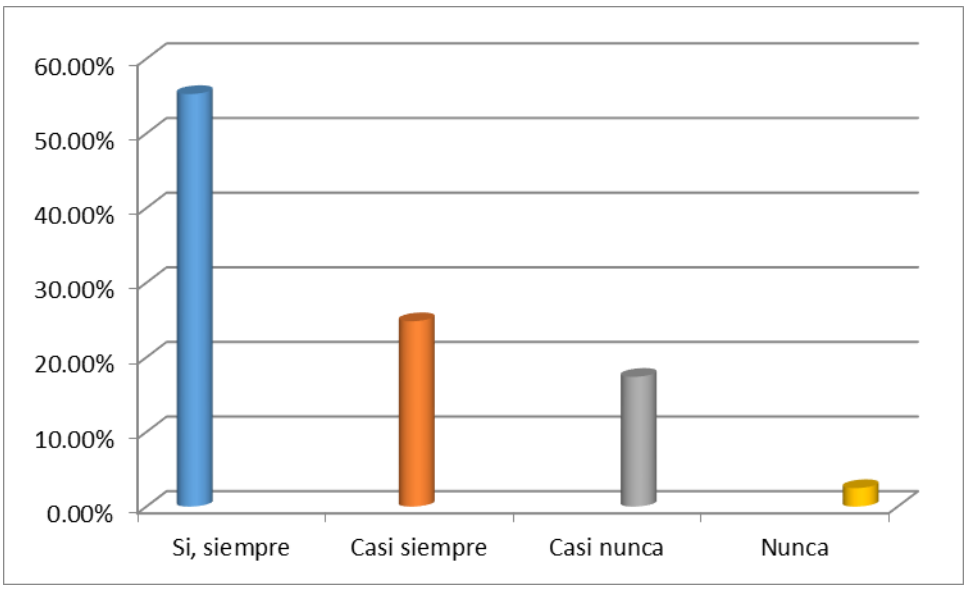
Alternativa	Muestra	%
Si, siempre	89	55.28
Casi siempre	40	24.84
Casi nunca	28	17.39
Nunca	4	2.48
Total	161	100.00

Fuente: Encuesta realizada entre el 1 y 12 de mayo del 2017

INTERPRETACION

El 80.12% de los encuestados manifiesta que siempre o casi siempre la certificación digital ayudaría a reducir la burocracia. Asimismo, el 13.72% considera que nunca o casi nunca la reduciría.

Gráfico Nº 14



A la pregunta:

15. ¿Con la certificación digital el sector privado agilizaría los trámites electrónicos que realiza con las instituciones del Estado?

    Se obtuvo el siguiente resultado:

Tabla Nº 15

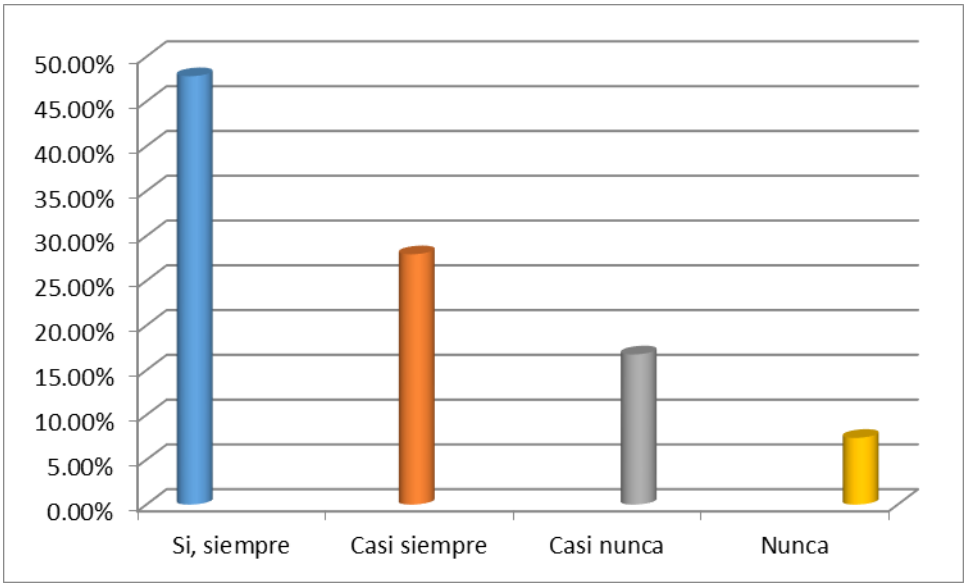
Alternativa	Muestra	%
Si, siempre	77	47.83
Casi siempre	45	27.95
Casi nunca	27	16.77
Nunca	12	7.45
Total	161	100.00

Fuente: Encuesta realizada entre el 1 y 12 de mayo del 2017

INTERPRETACION

El 75.78% de los encuestados manifiesta que siempre o casi siempre se agilizarían los trámites electrónicos que el sector privado realiza con el Estado. Asimismo, el 24.22% manifiesta que nunca o casi nunca lo agilizaría.

Gráfico Nº 15



A la pregunta:

16. ¿Considera usted que con la certificación digital las empresas privadas reducirían sus costos en las transacciones que realizan?

    Se obtuvo el siguiente resultado:

Tabla Nº 16

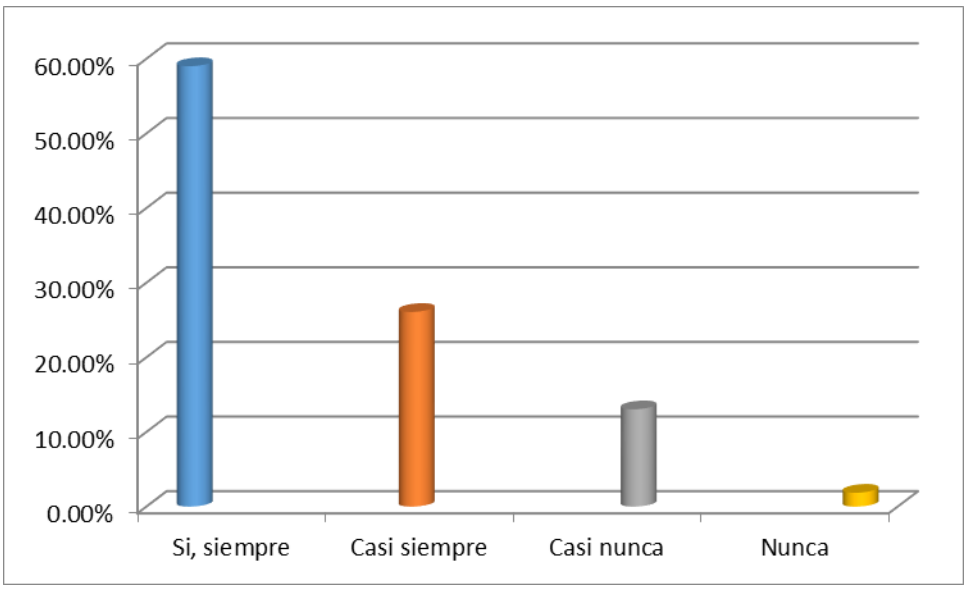
Alternativa	Muestra	%
Si, siempre	95	59.01
Casi siempre	42	26.09
Casi nunca	21	13.04
Nunca	3	1.86
Total	161	100.00

Fuente: Encuesta realizada entre el 1 y 12 de mayo del 2017

INTERPRETACION

El 85.10% de los encuestados considera que siempre y casi siempre la certificación digital reduciría los costos de las transacciones. El 14.90% considera que nunca o casi nunca lo reduciría.

Gráfico Nº 16



A la pregunta:

17. ¿Considera usted una buena alternativa implementar la certificación digital en la institución donde labora?

Se obtuvo el siguiente resultado:

Tabla Nº 17

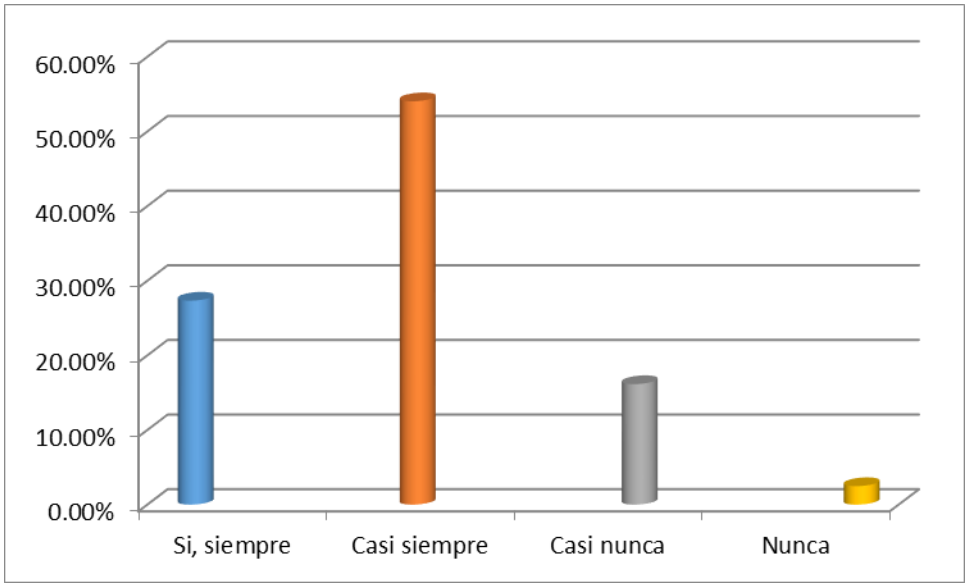
Alternativa	Muestra	%
Si, siempre	44	27.33
Casi siempre	87	54.04
Casi nunca	26	16.15
Nunca	4	2.48
Total	161	100.00

Fuente: Encuesta realizada entre el 1 y 12 de mayo del 2017

INTERPRETACION

El 81.37% de los encuestados manifiesta que siempre o casi siempre implementar la certificación digital es una buena alternativa. Asimismo, el 18.63% considera que nunca o casi nunca sería una buena alternativa.

Gráfico Nº 17



A la pregunta:

18. ¿La implementación de la certificación digital, permitiría una gestión administrativa eficiente en las instituciones del estado peruano?

    Se obtuvo el siguiente resultado:

Tabla Nº 18

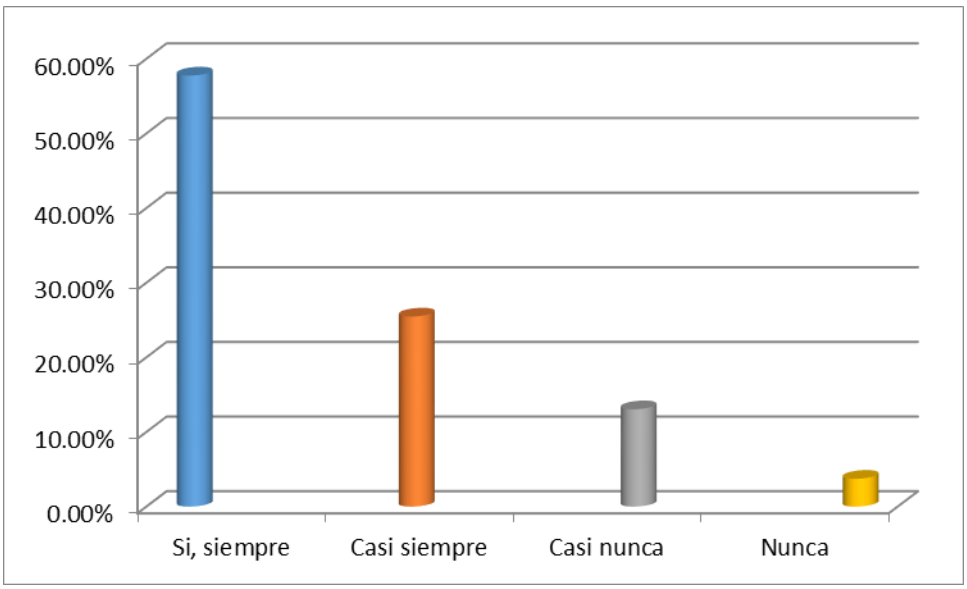
Alternativa	Muestra	%
Si, siempre	93	57.76
Casi siempre	41	25.47
Casi nunca	21	13.04
Nunca	6	3.73
Total	161	100.00

Fuente: Encuesta realizada entre el 1 y 12 de mayo del 2017

INTERPRETACION

El 83.23% de los encuestados manifiesta que siempre o casi siempre la implementación de la certificación digital, permitiría una gestión administrativa eficiente. El 16.77% manifiesta que nunca o casi nunca lo permitiría.

Gráfico Nº 18



4.2 CONTRASTACION DE HIPOTESIS

La contrastación de la hipótesis supone una serie de aspectos. Un primer aspecto es tener en cuenta dos tipos de hipótesis, la hipótesis alternativa y la hipótesis nula. La contrastación se ha realizado solamente con la hipótesis principal, porque las hipótesis secundarias son derivadas de la hipótesis principal.

Hipótesis Alternativa:

H1: La implementación de la certificación digital, permitiría una gestión administrativa eficiente en las instituciones del estado peruano.

En cambio la hipótesis nula es la siguiente:

H0: La implementación de la certificación digital, NO permitiría una gestión administrativa eficiente en las instituciones del estado peruano.

CONTRASTACIÓN ESTADÍSTICA:

La hipótesis estadística es una afirmación respecto a las características de la población. Contrastar una hipótesis es comparar las predicciones realizadas por el investigador con la realidad observada. Si dentro del margen de error que se ha admitido 5.00%, hay coincidencia, se acepta la hipótesis y en caso contrario se rechaza. Este es el criterio fundamental para la contrastación. Este es un criterio generalmente aceptado en todos los medios académicos y científicos.

Existen muchos métodos para contrastar las hipótesis. Algunos con sofisticadas fórmulas y otros que utilizan modernos programas informáticos. Todos de una u otra forma explican la forma como es posible confirmar una hipótesis.

En este trabajo se ha utilizado el software SPSS por su versatilidad y comprensión de los resultados obtenidos.

Para efectos de contrastar la hipótesis es necesario disponer de los datos de las variables: Independiente y dependiente.

La variable independiente es **CERTIFICACIÓN DIGITAL** y la variable dependiente es **GESTIÓN ADMINISTRATIVA.**

Los resultados del Sistema SPSS, son los siguientes:

TABLA DE ESTADÍSTICOS:

ESTADÍSTICOS		**CERTIFICACIÓN DIGITAL**	**GESTIÓN ADMINISTRATIVA**
Muestra	Válidos	161	161
	Perdidos	000	000
Media		92.88	95.08
Mediana		97.08	96.08
Moda		98.00	98.00
Desviación típica.		6.38	4.48
Varianza		40.88	19.68
Mínimo		84.00	88.00
Máximo		98.00	100.00

Fuente: Encuesta realizada

ANÁLISIS DE LA TABLA DE ESTADÍSTICOS:

En esta tabla se presentan los estadísticos más importantes.

La media o valor promedio de la variable independiente es 92.88% en cambio la media o promedio de la variable dependiente es 95.08%. Lo que indica un buen promedio para ambas variables, siendo mejor para la variable dependiente, que es la que se busca solucionar, lo cual apoya el modelo de investigación llevado a cabo.

La desviación típica mide el grado de desviación de los valores en relación con el valor promedio, en este caso es 6.38% para la variable independiente y 4.48% para la variable dependiente, lo que quiere decir que hay alta concentración en los resultados obtenidos; siendo mejor dicha concentración en la variable dependiente, lo que favorece al modelo de investigación propuesto.

TABLA DE CORRELACIÓN ENTRE LAS VARIABLES:

VARIABLES DE LA INVESTIGACION	INDICADORES ESTADÍSTICOS	CERTIFICACIÓN DIGITAL	GESTIÓN ADMINISTRATIVA
CERTIFICACIÓN DIGITAL	Correlación de Pearson	100%	**79.48%**
	Sig. (bilateral)		**3.38%**
	Muestra	153	153
GESTIÓN ADMINISTRATIVA	Correlación de Pearson	**79.48%**	100%
	Sig. (bilateral)	**3.38%**	
	Muestra	161	161

Fuente: Encuesta realizada

ANÁLISIS DE LA TABLA DE CORRELACIÓN ENTRE VARIABLES:

Esta tabla mide el grado de relación entre las variables independiente y dependiente. Dentro de ello el coeficiente de correlación y el grado de significancia.

La correlación se mide mediante la determinación del Coeficiente de correlación. R = Coeficiente de correlación. Este método mide el grado de relación existente entre dos variables, el valor de R varía de -1 a 1.

En la presente investigación el valor de la correlación es igual a 0.7948, es decir 79.48%, lo cual indica correlación directa (positiva), regular, por tanto aceptable.

La prueba de significancia estadística busca probar que existe una diferencia real, entre dos variables estudiadas, y además que esta diferencia no es al azar. Siempre que se estudie dos diferencias existe la probabilidad que dichas diferencias sean producto del azar y por lo tanto deseamos conocerlo y para ello usamos la probabilidad que no es más que el grado de significación estadística, y suele representarse con la letra p.

El valor de p es conocido como el valor de significancia. Cuanto menor sea la p, es decir, cuanto menor sea la probabilidad de que el azar pueda haber producido los resultados observados, mayor será la tendencia a concluir que la diferencia existe en realidad. El valor de p menor de 0.05 nos indica que el investigador acepta que sus resultados tienen un 95% de probabilidad de no ser producto del azar, en otras palabras aceptamos con un valor de p = 0.05, que podemos estar equivocados en un 5%.

Ahora en base al cuadro del SPSS tenemos un valor de significancia (p), igual a 3.30%, el mismo que es menor al margen de error propuesto del 5.00%, lo que, de acuerdo con la teoría estadística generalmente aceptada, permite rechazar la hipótesis nula y aceptar la hipótesis alternativa, desde el punto de vista de la correlación de las variables.

Luego, esto significa que la correlación obtenida para la muestra es significativa y que dicho valor no se debe a la casualidad, sino a la lógica y sentido del modelo de investigación formulado; todo lo cual queda consolidado con la tabla de regresión.

TABLAS DE REGRESIÓN DEL MODELO:

VARIABLES INTRODUCIDAS/ELIMINADAS:

Modelo	Variables introducidas	Variables eliminadas	Método
1	**CERTIFICACIÓN DIGITAL** **GESTIÓN ADMINISTRATIVA**	0	estadístico

Fuente: Encuesta realizada.

RESUMEN DEL MODELO DE LA INVESTIGACION:

Modelo	R	R cuadrado	R cuadrado corregida	Error típico de la estimación
1	79.48% (a)	93.18%	75.78%	2.98%

Fuente: Encuesta realizada.

ANÁLISIS DE LA TABLA DE REGRESIÓN:

La Regresión como la correlación son dos técnicas estadísticas que se pueden utilizar para solucionar problemas comunes en diversos aspectos del quehacer humano. Muchos estudios se basan en la creencia de que es posible identificar y cuantificar alguna Relación Funcional entre dos o más variables, donde una variable depende de la otra variable.

La regresión es una técnica estadística generalmente aceptada que relaciona la variable dependiente **GESTIÓN ADMINISTRATIVA** con la información suministrada por otra variable independiente **CERTIFICACIÓN DIGITAL**

El cuadro del Modelo presenta el Coeficiente de correlación lineal corregido 75.78%, el cual, pese al ajuste que le da el sistema, significa una correlación aceptable.

El Modelo o Tabla de Regresión también nos proporciona el Coeficiente de Determinación Lineal (R cuadrado = 93.18%. De acuerdo al coeficiente de determinación obtenido el modelo de regresión explica que el 93.18% de la variación total se debe a la variable independiente: **CERTIFICACIÓN DIGITAL** y el resto se atribuye a otros factores; lo cual tiene lógica, por cuanto además de este instrumento hay otros elementos que pueden incidir en la variable dependiente **GESTIÓN ADMINISTRATIVA.**

El Modelo también presenta el valor del Coeficiente de Correlación (R), igual al 79.48%, que significa una correlación buena en el marco de las reglas estadísticas generalmente aceptada.

Finalmente la Tabla de Regresión presenta el Error típico de Estimación, el mismo que es igual al 2.98%. Dicho valor es la expresión de la desviación típica de los valores observados respecto de la línea de regresión, es decir, una estimación de la variación probable al hacer predicciones a partir de la ecuación de regresión. Es un

resultado que favorece al modelo de investigación desarrollado, debido a que está por debajo del margen de error considerado del 5.00%.

TABLA DE ANÁLISIS DE VARIANZA-ANOVA:

Modelo		Suma de cuadrados	gl	Media cuadrática	F	Sig.
1	Regresión	74.438%	1	74.438%	8.548%	3.38%
	Residual	43.568%	5	8.718%		
	Total	118.006%	6			

Fuente: Encuesta realizada

ANÁLISIS DE LA TABLA ANOVA:

La varianza es una característica de la muestra que cuantifica su dispersión o variabilidad en relación del valor promedio. La varianza tiene unidades al cuadrado de la variable. Su raíz cuadrada positiva es la desviación típica. Ahora, ANOVA, son las siglas de Análisis de la Varianza y la misma es una técnica estadística que sirve para decidir / determinar si las diferencias que existen entre las medidas de las variables son estadísticamente significativas. El análisis de varianza, es uno de los métodos estadísticos más utilizados y más elaborados en la investigación moderna.

La técnica ANOVA se ha desarrollado para el análisis de datos en diseños estadísticos como el presente.

El valor más importante para efectos del trabajo es el Valor sig = 3.38%. Ahora comparando el margen de error del 5.00% propuesto y el valor de significancia, p=3.38%, tenemos que este último es menor. Por tanto, de acuerdo a la doctrina estadística generalmente aceptada, se concreta en el rechazo de la hipótesis nula y

en la aceptación de la hipótesis del investigador. Lo que de otro modo, significa también que se acepta el modelo obtenido a partir de la muestra considerada.

TABLA DE COEFICIENTES (a):

Modelo	Variables	Coeficientes no estandarizados		Coeficientes estandarizados	t	Sig.
		B	Error típ.	Beta	B	Error típ.
1	**CERTIFICACIÓN DIGITAL**	43.80%	17.55%		2.50 %	**3.88%**
	GESTIÓN ADMINISTRATIVA	55.10%	18.90%	79.40%	2.92 %	**3.28%**

Fuente: Encuesta realizada

ANÁLISIS DE LA TABLA DE COEFICIENTES:

La columna de mayor relevancia está referida al Grado de significancia, que el sistema SPSS, lo presenta como sig. El grado de significancia se compara con el denominado margen de error propuesto, en el presente caso: 5.00% y se establece la contrastación de la hipótesis. El valor del Grado de significancia obtenido en la tabla, para el caso de la variable dependiente **GESTIÓN ADMINISTRATIVA** es 3.28%, luego este valor es menor que el margen de error del 5.00% propuesto, entonces se concluye que a un nivel de significancia del 3.28% se rechaza la hipótesis nula y se acepta la hipótesis alternativa.

En el caso de la Variable Independiente **CERTIFICACIÓN DIGITAL** se tiene que el valor de p = 3.88%, al igual que en el caso anterior, también es menor que el margen de error del 5.00% propuesto por el investigador; por tanto se concluye que a un nivel de significancia propuesto del 3.88% se rechaza la hipótesis nula y se acepta la hipótesis alternativa.

CAPITULO V

DISCUSION

5.1 DISCUSIÓN

a) El 82.23% de los encuestados considera que siempre o casi siempre la implementación de la certificación digital, permitiría una gestión administrativa eficiente en las instituciones del estado peruano. Este resultado es similar al presentado, aunque en otra dimensión espacial y temporal, por Aguilar Alcarráz Gino Brehan (2016) “Implementación de un modelo simplificado de firma digital basado en la tecnología PKI y la invocación por protocolos caso de estudio: municipalidad de Miraflores”. Ambos resultados son razonables y por tanto favorecen la investigación desarrollada.

b) El 82.23% de los encuestados manifiesta que siempre y casi siempre identificarse electrónicamente a través de la certificación digital, permitiría una gestión administrativa eficiente en las instituciones del estado peruano. Este resultado es similar al presentado, aunque en otra dimensión espacial y temporal, por Reyes Krafft, Alfredo Alejandro (2002) “La firma electrónica y las entidades de certificación”. Ambos resultados son razonables y por tanto favorecen la investigación desarrollada.

c) El 81.99% de los encuestados manifiesta que siempre y casi siempre la protección de la información a través de la certificación digital, permitiría una gestión administrativa eficiente en las instituciones del estado peruano. Este

resultado es similar al presentado, aunque en otra dimensión espacial y temporal, por Viega Rodríguez, María José y Rodríguez Acosta, Beatriz (2005) "Documento electrónico y firma digital, cuestiones de seguridad en las nuevas formas documentales". Ambos resultados son razonables y por tanto favorecen la investigación desarrollada.

d) El 83.85% de los encuestados considera que siempre y casi siempre garantizar la integridad de la información a través de la certificación digital, permitiría una gestión administrativa eficiente en las instituciones del estado peruano. Este resultado es similar al presentado, aunque en otra dimensión espacial y temporal, por García Rojas Walter Augusto (2008) "Implementación de firma digital en una plataforma de comercio electrónico". Ambos resultados son razonables y por tanto favorecen la investigación desarrollada.

CONCLUSIONES

1. La investigación ha podido determinar a través de una serie de preguntas que el 75.15% de los encuestados realizan transacciones electrónicas bastante y regularmente. Asimismo, dedican semanalmente entre 4 a 6 horas de su tiempo en transacciones electrónicas (51.55%)

2. Se ha logrado determinar que, el 84.47% de los encuestados manifiesta que siempre o casi siempre los mecanismos de protección de la certificación digital son seguros.

3. Se estableció que, los encuestados consideran que siempre o casi siempre la certificación digital, permitiría una gestión administrativa eficiente, que incrementarían las transacciones electrónicas, y que difundir los mecanismos permitiría que más usuarios utilicen la certificación digital.

4. El estudio demuestra que, el 75.78% de los encuestados manifiesta que la certificación digital agilizaría los trámites electrónicos que el sector privado realiza con el Estado. Asimismo, el 85.10% de los encuestados considera que la certificación digital reduciría los costos de las transacciones

5. También se demuestra que, el 83.23% de los encuestados manifiesta que siempre o casi siempre la implementación de la certificación digital, permitiría una gestión administrativa eficiente en las instituciones del estado peruano.

RECOMENDACIONES

1. Se deben fomentar políticas públicas que faciliten la interacción de los usuarios con las instituciones del estado y realicen mayores horas de transacciones electrónicas semanales.

2. Es necesario difundir que la herramienta de certificación digital es bastante segura, para así poder lograr incrementar la participación de los ciudadanos en las transas acciones que realizan con las instituciones del estado.

3. Deben reformularse los protocolos administrativos en las instituciones del estado para permitir una gestión administrativa eficiente que genere una atención de calidad a los usuarios.

4. Implementar un programa que fortalezca la relación instituciones del estado-usuarios que permitirían una mejor utilización de los fondos del sistema de certificación digital.

5. Impulsar la masificación de la certificación digital en las transacciones electrónicas, lo cual permitiría una sinergia que beneficiaría a toda la sociedad peruana.

REFERENCIAS BIBLIOGRÁFICAS

Aguilar**,** Gino. (2016). *Implementación de un modelo simplificado de firma digital basado en la tecnología PKI y la invocación por protocolos caso de estudio: municipalidad de Miraflores.* (Tesis de grado, Universidad Nacional Mayor de San Marcos). Lima.

Areitio**,** J. (2008). *Seguridad de la información: redes, informática y sistemas de información*., Editorial Paraninfo .Madrid.

Barrios, G. y otros, (1999). *Internet y Derecho en México.* Editorial Mc. Graw Hill, México.

Basurto, A. (2015). *Aspectos de seguridad de Bitcoin y su aplicación en una alternativa de infraestructura de llave pública*. (Tesis de maestría, Centro de Investigación y de Estudios Avanzados del Instituto Politécnico Nacional)

Barzallo, J. (2008). *La firma digital*, Quito. En: sbarzal@uio.satnet.net

Bravo, A. (2001). *Seguridad en transacciones por internet*. (Tesis de grado, Universidad Panamericana).

Cánovas, O. (2002). *Propuesta de una Infraestructura de Clave Pública y su Extensión Mediante un Sistema de Gestión Distribuida de Credenciales Basado en Delegación y Roles.* (Tesis de doctorado, Universidad de Murcia).

Castells, M. (1989). *La ciudad informacional: tecnologías de información, reestructuración económica y el proceso urbano-regional*. Alianza. Madrid

Chiriboga, R. (2014). *El impacto social y la incidencia que tiene el uso de la firma electrónica (Token) en los pequeños y medianos exportadores ecuatorianos*. (Tesis de grado, Universidad de las Fuerzas Armadas).

Contreras, I. (2009). *La firma electrónica y la función notarial en Jalisco*. (Tesis de maestría, Universidad de Guadalajara).

Esteban, M. (2001). *Delitos Cibernéticos*. (Tesis de grado, Universidad Panamericana

España, M. (2003), *Servicios Avanzados de Telecomunicación.* Editorial Díaz de Santos, Madrid.

García, W. (2008). *Implementación de Firma Digital en una Plataforma de Comercio Electrónico*. (Tesis de grado, Pontificia Universidad Católica del Perú).

Indecopi (2007). *Guía de Acreditación de Entidades de Certificación EC.Versión 3.3* IOFE, Lima

Jordan, T. (1999). *Cyberpower: la cultura y la política del ciberespacio e Internet*. Aldrubal. Londres:

Lakatos, I. (1983). *La metodología de los programas de investigación científica*. Alianza, Madrid

Levy, S. (2001). *Hackers: Héroes de la revolución informática*. Penguin. Nueva York

Lievwrouw, L. (2012). *La próxima década en el tiempo de Internet*. Information, Communication & Society, Madrid

Mariño, A. (2010). *Factores inhibidores en la implementación de sistemas de gestión de la seguridad de la información basado en la NTP-ISO/IEC 17799 en la administración pública*. (Tesis de maestría, Universidad Nacional Mayor de San Marcos).

Martínez, A. (2000). *La contratación Jurídica a través de medios electrónicos*. (Tesis de grado, Universidad Panamericana).

Matos, N. (2006). *La piratería: ¿problema o solución?*. Documento de trabajo de ESAN. Lima

Mattelart, A. (2002). *Historia de la sociedad de la información*. Paidós. Barcelona:

Ministerio de Transportes y Comunicaciones (2011). *Plan nacional para el desarrollo de la banda ancha en el Perú*. En: http://www.mtc.gob.pe/portal/proyecto_banda_ancha/Plan%20Banda%20Ancha%20vf.pdf.

Montesinos, A. (1999). *La Sociedad de la Información e Internet*. Editorial San Pablo. España.

ONGEI (2002). *Infraestructura de Llave Pública para el Estado Peruano (PKI) Framework.* Recuperado de: http://www.ongei.gob.pe/publica/proyectos/4821.pdf).

ONGEI (2013). *Política Nacional de Gobierno Electrónico 2013-2017*. Recuperado de: http://www.ongei.gob.pe/docs/Pol%C3%ADtica_Nacional_de_Gobierno_Electronico_2013_2017.pdf)

Orozco, R. (2011). *Diseño e implementación de un módulo de facturación electrónica para el hospital San José satélite*. (Tesis de maestria, Instituto Politécnico Nacional)

Paquet, J. y Saxe, W. (2004). *The Business Case for Network Security: Advocacy*, Governance, and ROI, Paidos, Boston

Pinela, E. (2013). *Análisis de la necesidad de la firma digital en las exportadoras e importadoras guayaquileñas para la creación de una empresa de certificación*. (Tesis de grado, Universidad de Guayaquil).

Rama, C. (2003). *Economía de las industrias culturales en la globalización digital*. Eudeba. Buenos Aires

Reyes, A. (2002). *La firma electrónica y las entidades de certificación*. (Tesis de doctor, Universidad Panamericana).

Rodríguez, M. (2011). *La firma electrónica y la fe pública*. (Tesis de grado, Universidad Autónoma de Queretaro).

Santizo, J. (2010). *Implementación y adopción de la firma electrónica en Guatemala*, (Tesis de grado, Universidad de San Carlos de Guatemala).

Stroke, P. (2000). *La Firma Electrónica*, Editorial Cono Sur, España

INAP. (2003). *Firma Digital y Administraciones Públicas*, Editorial Paraninfo, Madrid.

Urbina, C. (2012). *Certificación para la digitalización de documentos en Chile*. (tesis de grado, Universidad de Chile).

Valdiviezo, T. (2012). *Análisis de la tecnología PKI y su aplicación en el aseguramiento de los servicios corporativos www, ftp y http*. (Tesis de grado, Escuela superior politécnica de Chimborazo).

Vernet, T. (2003). *Firma digital*, (Tesis de grado, Universidad abierta interamericana, Buenos Aires).

Viega, M. y Rodríguez, B. (2005). *Documento electrónico y firma digital, cuestiones de seguridad en las nuevas formas documentales*. Instituto de derecho

informático de la facultad de derecho de la Universidad de la República de Uruguay, Montevideo

Villalobos A. (1998). *En Panamá: ¿está protegida la intimidad por violaciones a través de la informática?*; Encuentros sobre Informática y Derecho; Universidad Pontificia Comillas, Madrid.

Villanueva, E. (2010). *Vida digital: la tecnología en el centro de lo cotidiano*. PUCP. Lima

Villanueva, E. (2015). *La incursión digital y la política pública: nuevos actores a partir del conflicto del derecho de autor en el campo digital*. (Tesis de doctor, Pontificia Universidad Católica del Perú).

Webtrust, F. (2011). *Trust Service Principles and Criteria for Certification Authorities Version 2.0* En: http://www.webtrust.org/homepage-documents/item54279.pdf

ANEXOS

ANEXO N° 01: MODELO DE ENCUESTA

"LA CERTIFICACION DIGITAL Y LA GESTIÓN ADMINISTRATIVA EFICIENTE EN LAS INSTITUCIONES DEL ESTADO PERUANO"

Datos generales de la persona encuestada
Nombre:
Cargo:
Lugar:
Fecha:

Nota importante: Favor contestar las siguientes preguntas marcando una alternativa o llenando los espacios en blanco, según corresponda.

1. ¿Usted realiza transacciones electrónicas?

   a) Muy poco ☐
   b) Poco ☐
   c) Regular ☐
   d) Bastante ☐

2. Cuantas horas semanales ocupa su tiempo en transacciones electrónicas:

   a) Menor a 2 horas ☐
   b) Mayor a 2 y menor a 4 ☐
   c) Mayor a 4 y menor a 6 ☐
   d) Mayor a 6 ☐

3. ¿Entiende las diferencias entre certificado digital y firma digital?

   a) Sí, siempre ☐
   b) Casi siempre ☐
   c) Casi nunca ☐
   d) Nunca ☐

4. ¿Considera que la certificación digital es un requisito indispensable para que las instituciones ofrezcan un servicio seguro a través de internet?

   a) Sí, siempre ☐
   b) Casi siempre ☐
   c) Casi nunca ☐
   d) Nunca ☐

5. ¿Conoce las ventajas de la certificación digital?

a) Sí, siempre ☐
b) Casi siempre ☐
c) Casi nunca ☐
d) Nunca ☐

6. ¿Identificarse electrónicamente a través de la certificación digital, permitiría una gestión administrativa eficiente en las instituciones del estado peruano?

a) Sí, siempre ☐
b) Casi siempre ☐
c) Casi nunca ☐
d) Nunca ☐

7. ¿Considera que los mecanismos de protección de la certificación digital son seguros?

a) Sí, siempre ☐
b) Casi siempre ☐
c) Casi nunca ☐
d) Nunca ☐

8. ¿Cree usted que la seguridad de los mecanismos de protección de la información a través de la certificación digital lograría incrementar las transacciones electrónicas?

a) Sí, siempre ☐
b) Casi siempre ☐
c) Casi nunca ☐
d) Nunca ☐

9. ¿Difundir los mecanismos de protección de la información permitiría que más usuarios utilicen la certificación digital?

a) Sí, siempre ☐
b) Casi siempre ☐
c) Casi nunca ☐
d) Nunca ☐

10. ¿La protección de la información a través de la certificación digital, permitiría una gestión administrativa eficiente en las instituciones del estado peruano?

a) Sí, siempre ☐
b) Casi siempre ☐
c) Casi nunca ☐
d) Nunca ☐

11. ¿Considera que la información a través de la certificación digital puede ser vulnerada?

a) Sí, Siempre ☐
b) Casi siempre ☐
c) Casi nada ☐
d) Nada ☐

12. ¿La integridad de la información a través de la certificación digital evitaría la falsificación de la información digital de las personas?

a) Sí, siempre ☐
b) Casi siempre ☐
c) Casi nunca ☐
d) Nunca ☐

13. ¿Garantizar la integridad de la información a través de la certificación digital, permitiría una gestión administrativa eficiente en las instituciones del estado peruano?

a) Sí, siempre ☐
b) Casi siempre ☐
c) Casi nunca ☐
d) Nunca ☐

14. ¿Considera usted que la certificación digital ayudaría a reducir la burocracia en las instituciones del estado?

a) Sí, siempre ☐
b) Casi siempre ☐
c) Casi nunca ☐
d) Nunca ☐

15. ¿Con la certificación digital el sector privado agilizaría los trámites electrónicos que realiza con las instituciones del Estado?

a) Sí, siempre ☐
b) Casi siempre ☐
c) Casi nunca ☐
d) Nunca ☐

16. ¿Considera usted que con la certificación digital las empresas privadas reducirían sus costos en las transacciones que realizan?

a) Sí, siempre ☐
b) Casi siempre ☐
c) Casi nunca ☐
☐

d) Nunca

17. ¿Considera usted una buena alternativa implementar la certificación digital en la institución donde labora?

a) Sí, siempre ☐
b) Casi siempre ☐
c) Casi nunca ☐
d) Nunca ☐

18. ¿La implementación de la certificación digital, permitiría una gestión administrativa eficiente en las instituciones del estado peruano?

a) Sí, siempre ☐
b) Casi siempre ☐
c) Casi nunca ☐
d) Nunca ☐

ANEXO N° 2:
MATRIZ DE CONSISTENCIA:
LA CERTIFICACION DIGITAL Y LA GESTIÓN ADMINISTRATIVA EFICIENTE EN LAS INSTITUCIONES DEL ESTADO PERUANO

PROBLEMAS	OBJETIVOS	HIPOTESIS	VARIABLES E INDICADORES
PROBLEMA PRINCIPAL ¿Permite, la implementación de la certificación digital, una gestión administrativa eficiente en las instituciones del estado peruano? **PROBLEMAS SECUNDARIOS** ¿Permite la identificación electrónica a través de la certificación digital, una gestión administrativa eficiente en las instituciones del estado peruano? ¿Permite la protección de la información a través de la certificación digital, una gestión administrativa eficiente en las instituciones del estado peruano? ¿Permite la garantía de la integridad de la información a través de la certificación digital, una gestión administrativa eficiente en las instituciones del estado peruano?	**OBJETIVO GENERAL** Demostrar que la implementación de la certificación digital, permitiría una gestión administrativa eficiente en las instituciones del estado peruano **OBJETIVOS ESPECIFICOS** Establecer si identificarse electrónicamente a través de la certificación digital, permitiría una gestión administrativa eficiente en las instituciones del estado peruano Entender si la protección de la información a través de la certificación digital, permitiría una gestión administrativa eficiente en las instituciones del estado peruano Determinar si garantizar la integridad de la información a través de la certificación digital, permitiría una gestión administrativa eficiente en las instituciones del estado peruano	**HIPÓTESIS GENERAL** La implementación de la certificación digital, permitiría una gestión administrativa eficiente en las instituciones del estado peruano **HIPÓTESIS ESPECÍFICAS** Identificarse electrónicamente a través de la certificación digital, permitiría una gestión administrativa eficiente en las instituciones del estado peruano La protección de la información a través de la certificación digital, permitiría una gestión administrativa eficiente en las instituciones del estado peruano Garantizar la integridad de la información a través de la certificación digital, permitiría una gestión administrativa eficiente en las instituciones del estado peruano	**Variable Independiente: Certificación digital** Indicadores: Reportes sobre implementación de la certificación digital. Cronograma de ejecución de la certificación digital. Ratios de avances de la certificación digital. **Variable Dependiente: Gestión administrativa** Indicadores: Reportes de gestión administrativa. Ratios de atención a los usuarios de la institución. Indicadores de atención de reclamos.