UNIVERSIDAD CÉSAR VALLEJO

ESCUELA DE POSGRADO

PROGRAMA ACADÉMICO DE MAETRÍA EN GESTIÓN PÚBLICA

La firma electrónica y la seguridad digital en los certificados de vigencia de poder emitidos por la Oficina Registral de Andahuaylas, 2022

TESIS PARA OBTENER EL GRADO ACADÉMICO DE:
Maestro en Gestión Pública

AUTOR:
Sotelo Cárdenas, Julio César (orcid.org/0000-0002-9612-2381)

ASESOR:
Dr. Osorio Carrera, Cesar Javier (orcid.org/0000-0002-2850-6420)

CO-ASESORA:
Mgs. Agreda Romero, Lourdes Zhuleim (orcid.org/0000-0003-2812-4817)

LÍNEA DE INVESTIGACIÓN:
Reforma y Modernización del Estado

LÍNEA DE RESPONSABILIDAD SOCIAL UNIVERSITARIA:
Fortalecimiento de la democracia, liderazgo y ciudadanía

TRUJILLO – PERÚ
2023

DEDICATORIA

La vida es un caminar constante y se vuelve fácil cuando tienes a tu alrededor maravillosos seres que dan lo mejor en cada momento; en mi vida he tenido la suerte de tener muchas personas las que me saben demostrar esto; Dios, el mejor de mis amigos, la luz que ilumina mi camino en tiempos oscuros y la fortaleza que me mantiene construyendo mis sueños, mis padres: César Leonardo Sotelo Quito y Gladys Cárdenas Zarzo, por su ejemplo, ternura y amor infinito que me enseñaron el verdadero sentido de la vida y que siempre me con su ejemplo me mostraron que hay mayor recompensa para los mayores esfuerzos, también gracias a mi hermano Marco Antonio Sotelo Cárdenas que con su apoyo incondicional me dio la seguridad para trabajar juntos por un futuro mejor.

A todos los familiares, amigos, maestros y conocidos no mencionados; personas maravillosas con quienes construí sueños e historias que vivirán y permanecerán en mi mente y corazón por siempre.

A todos ellos, tengo un aprecio y gratitud infinitos.

AGRADECIMIENTO

Al culminar con el presente trabajo de investigación deseo agradecer de manera muy especial a todos los docentes que ayudaron en mi formación académica la cual me permite decir que ahora entiendo mejor el sector público, también agradecer a mis amigos y familiares puesto que merecen una disculpa plena por tantas ausencias.

A la Oficina Registral de Andahuaylas que me permitió y me dio las facilidades para poder desarrollar esta investigación.

ÍNDICE DE CONTENIDOS

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

RESUMEN

La presente investigación busca analizar y comprender el nivel de correlación que existe entre la seguridad digital y el tipo de firma electrónica utilizados para la emisión de certificados de vigencia de poder de la Oficina Registral de Andahuaylas, dado que estos certificados son de mucha utilidad a nivel comercial como personal, puesto que facilitan la representación de las personas naturales y/o jurídicas en la celebración de actos y contratos.

Al analizar una muestra de 70 certificados de vigencia de poder emitidos por la oficina Registral de Andahuaylas se observó que poseen un nivel de seguridad medio bajo y resulta muy fácil su adulteración parcial y/o total. Con lo que poder sorprender a personas y/o instituciones con un certificado distinto al original resulta bastante simple.

Todo lo mencionado surge por la utilización de un tipo de firma electrónica simple que no garantiza la intangibilidad del documento puesto que los mecanismos utilizados a la hora de realizar la firma electrónica mediante la incrustación de: imagen escaneada de la firma del abogado certificador, código QR, código de verificación, número y año de publicidad; en lugar de proteger el documento facilitan su adulteración.

Y por último al analizar la relación de las variables (seguridad digital y firma electrónica) se determinó que estas cuentan con una relación perfecta positiva ($\rho = 0{,}91701$), de lo cual se deduce que si se mejora el tipo de firma se mejorara el nivel de seguridad de los certificados de vigencia de poder emitidos por la oficina Registral de Andahuaylas; También se determinó que ambas variables cuentan con causalidad directa.

Palabras clave: Seguridad digital, firma electrónica, certificados de vigencia de poder, Ley de Certificado y Firma Digital No. 27269.

ABSTRACT

The present investigation seeks to analyze and understand the level of correlation that exists between digital security and the type of electronic signature used for the issuance of certificates of validity of power of the Andahuaylas Registry Office, given that these certificates are very useful at the national level. commercial and personal, since they facilitate the representation of natural and/or legal persons in the celebration of acts and contracts.

When analyzing a sample of 70 power of attorney certificates issued by the Andahuaylas Registry Office, it was observed that they have a medium-low security level and their partial and/or total adulteration is very easy. So being able to surprise people and/or institutions with a certificate other than the original is quite simple.

All of the aforementioned arises from the use of a type of simple electronic signature that does not guarantee the intangibility of the document since the mechanisms used when making the electronic signature by embedding: scanned image of the certifying lawyer's signature, QR code, verification code, number and year of advertising; Instead of protecting the document, they facilitate its adulteration.

And finally, when analyzing the relationship of the variables (digital security and electronic signature), it was determined that these have a perfect positive relationship (ρ=0.91701), from which it can be deduced that if the type of signature is improved, it will be improved. the security level of the power of attorney certificates issued by the Andahuaylas Registry office; It was also determined that both variables have direct causality.

Keywords: Digital security, electronic signature, power of attorney certificates, Digital Certificate and Signature Law No. 27269.

I. INTRODUCCIÓN

La llegada del COVID-19 lo ha cambiado todo, desde el 11 de marzo, cuando la Organización Mundial de la Salud declaró al COVID-19 como pandemia, se ha dado un giro importante en el codesarrollo de las actividades del día a día, que es la creciente adopción de herramientas tecnológicas por parte de organismos públicos y privados para asi continuar brindando los diferentes productos y servicios al público.

En el mundo entero se libra una batalla día a día con el fin de mantener la seguridad digital, la perdida de privacidad, la suplantación y el espionaje son algunos de los problemas más serios que enfrentamos en los diferentes rubros; ya sea al acceder a una aplicación, página web, dar nuestro consentimiento para realizar una trasferencia finiera, etc. Es por todo esto que cada vez se adoptan mejores mecanismos para ofrecer mayor seguridad digital a los usuarios.

Razón por la cual el mundo entero adopta los documentos digitales con firma electrónica, no siendo esto algo nuevo, ya que la primera ley sobre el uso y reglamentación de la firma electrónica logra su aprobación en 1995 en el condado de Utah, Estados Unidos (e-certchile, 2020). como mecanismo para que los diferentes usuarios puedan brindar consentimientos en ciertas operaciones realizadas a lo largo de su día a día.

En Estados Unidos, la ley ESIGN y la ley de Transacciones Electrónicas Uniformes (UETA por sus siglas en inglés) sentaron las bases legales para que la firma electrónica se pudiera utilizar en todos los estados.

En la Unión Europea, el Reglamento de Identificación Electrónica y Servicios de Confianza (eIDAS) estableció una ley que ayuda a normalizar las firmas electrónicas en todos los estados miembros.

Hasta ahora en América Latina, muchos gobiernos han estado apostando por la administración digital, lo que ha traído muchos beneficios. Esto es para regular y/o obligar a las empresas públicas y privadas a iniciar su transformación digital.

La automatización de procesos de facturación, financieros o contables conduce a la digitalización de otros procedimientos comerciales, como la firma de documentos. Las firmas digitales simplifican muchos pasos. No solo mejora la

gestión y el control de documentos, proporciona trazabilidad y transparencia, sino que también es un mecanismo de seguridad. Sin embargo, su uso no es común en las empresas latinoamericanas.

El propósito principal de las firmas electrónicas es proporcionar la misma validez legal que las firmas manuscritas. Por esta razón, cada país ha promulgado leyes específicas que establecen un conjunto de requisitos que rigen su uso.

Argentina fue uno de los primeros países de América Latina en regular las firmas electrónicas. La Ley de Firma No. 25506 fue promulgada en 2001 y entró en vigencia en 2007. La ley regula el uso de firmas digitales por parte de las agencias de empleo del sector público y privado. Su uso no se extendió a todas las empresas privadas hasta que entró en vigor el Decreto Ejecutivo 927/2014 en 2014. Asimismo, el Código Civil argentino establece que, para que una firma electrónica sea válida, el firmante debe haber celebrado previamente un contrato jurídicamente vinculante.

En Colombia, las firmas digitales en documentos están reguladas por la Ley N° 527 de 1999 y el Decreto N° 1747 de 2000. La primera ley que define y regula los requisitos de acceso y uso de los mensajes de datos, el comercio electrónico y las empresas. Organismo de Certificación Digital y Normativa. Una firma electrónica es legalmente lo mismo que una firma manuscrita. El artículo 7 establece que para cumplir con los mismos requisitos que las firmas electrónicas, las firmas digitales deben utilizarse para identificar al remitente de un mensaje de datos e indicar que su contenido fue aceptado por esa persona. Confiable y adecuado para el propósito para el cual se creó o comunicó el mensaje. En cuanto a los organismos de certificación, la Ley N° 527 de 1999 establece que los organismos de certificación son los encargados de emitir firmas digitales bajo el control y supervisión de la Dirección General de Industria y Comercio. El Decreto N° 1747 de 2000 define los organismos de acreditación.

Varias leyes regulan el uso de tres tipos de firmas electrónicas en México.

Firma electrónica simple: Tal como lo establece el artículo 89 del Código de Comercio, una firma electrónica se define como un conjunto de datos que identifica de manera única al firmante, tiene el mismo valor legal que una firma y se permite su uso como prueba de consulta.

Firmas Electrónicas Avanzadas: Definidas en la Sección 2 de la Ley de Firmas Electrónicas Avanzadas, brindan mayor seguridad que las firmas electrónicas simples. Para utilizar firmas digitales avanzadas, necesita un certificado digital de un proveedor de servicios de certificados.

Firma biométrica: Firma realizada por un firmante en un dispositivo electrónico. Tiene el mismo valor legal que una firma digital avanzada.

En Ecuador, las firmas electrónicas están reguladas por la Ley de Comercio Electrónico, Firmas e Información de Datos de abril de 2002, la cual fue reformada y ampliada en 2014. El reglamento establece los requisitos para el uso de firmas electrónicas por personas físicas y jurídicas. Para utilizarlo se necesita un certificado de firma electrónica emitido por el Banco Central del Ecuador. Una firma digital se refiere a un documento virtual compuesto por una cadena de códigos dentro de un período de tiempo determinado según las características y necesidades del firmante.

En Perú, esto comenzó con la Ley de Certificado y Firma Digital No. 27269 implementada por el Ministerio de Justicia y Derechos Humanos (MINJUSDH) en el año 2000 para simplificar, reducir costos y proteger los procesos y procedimientos entre los ciudadanos y el gobierno. (MINJUSDH, 2000)

La ley finalmente se reglamentó en 2008, y los primeros certificados digitales no se emitieron a personas jurídicas hasta 2012. Esto se debe a que el país no cuenta con la tecnología suficiente para implementarlo.

Actualmente, las firmas electrónicas se utilizan para firmar electrónicamente documentos de pago digitales, como facturas y recibos de ventas. Es una herramienta fundamental de la SUNAT para combatir la corrupción y aumentar la eficacia y eficiencia en el camino hacia el gobierno electrónico a través de la modernización del Estado. (LlamaPE, 2022).

Y es así que la Super Intendencia Nacional de los Registros Públicos SUNARP, adopta estos mecanismos tecnológicos para agregar seguridad a los certificados literales y de vigencia de poder la cual se aprueba y reglamenta mediante Resolución del Superintendente Nacional de los Registros Públicos Nº 058-2020-SUNARP/SN entrando en vigencia a partir del 08 de junio de 2020 para el caso

de los Registros de Propiedad Inmueble, Personas Jurídicas y Personas Naturales; mientras que a partir del 01 de julio de 2020 para el registro de Bienes Muebles. (SUNARP, 2020)

Y es así como hasta la fecha se vienen emitiendo los certificados de vigencia de poder por el área de publicidad registral de la Oficina Registral de Andahuaylas, esto sin contar que el certificado de vigencia de poder representa un poder concedido única y exclusivamente a el(los) apoderado(os) razón por la cual el certificado digital debe cumplir al menos 2 principios (Integridad y intangibilidad) durante el tiempo que este se encuentre vigente o la entidad receptora lo disponga, puesto que es un reproducción total o parcial del poder primigenio que la Super Intendencia Nacional de los Registros Públicos inscribió y por ende resguarda.

En la actualidad los certificados de vigencia de poder vienen siendo firmados por un tipo de firma electrónica la cual no permite brindar o asegurar los 2 principios antes mencionados puesto que es muy fácil la manipulación y adulteración de estos certificados e incluso la generación de un nuevo código QR que nos dirija al documento adulterado.

Todo esto sucede puesto que los sistemas para la emisión de certificados de vigencia de poder solo permiten la utilización de un determinado tipo de firma electrónica que no es más que una representación impresa de la firma manuscrita de abogado certificador y a esto se le agrego la validación por código QR que es igual de vulnerable.

Según lo descrito esto podría acarrear consecuencias muy grabes puesto que cualquier individuo podría suplantar al apoderado consignado en un determinado certificado de vigencia de poder y sorprender tanto a entidades públicas como privadas. Por ejemplo: Cristina Barrientos Apaza brinda poder a Juan Pérez Ortiz para vender una casa de 200 metros, el parte notarial que donde existe el poder se presenta a la Super Intendencia Nacional de los Registros Públicos la cual califica e inscribe dicha petición; al cabo de unos meses Ignacio Sanches Peláez se entera de esta situación y solicita el certificado de vigencia de poder de Juan Pérez Ortiz y adultera algunos datos contenidos en este (datos del apoderado básicamente) apareciendo esta vez como único apoderado Juan Pérez Ortiz y

realizando la posterior venta del inmueble en una notaría cualquiera presentando su certificado de vigencia de poder.

Con este estudio se pretende analizar y determinar las posibles causas de lo descrito anterior mente y de esta manera proponer alternativas de solución a las mismas.

Figura 1: *Seguridad digital y firma electrónica*

Fuente: (HOLVOET, 2020)

II. MARCO TEÓRICO

Firma electrónica: Cuando se trata de firmas electrónicas, es importante considerar su definición, del Sistema Europeo de Identificación Electrónica (conocido por las siglas en inglés eIDAS, Electronic Identification, Authentication and Trust Services) y su Reglamento (UE) N° 910/2014. Que entró en vigor en toda la Unión Europea el 1 de julio de 2016 especificando tres tipos de firmas electrónicas (eIDAS, 2014):

Firma electrónica simple: Se considera firma electrónica toda firma en la que el firmante acepta la condición del documento que firma. Esto se puede hacer a través de los esquemas de firma de nuestra computadora, botones para aceptar los términos del contrato, casillas de aceptación de derechos, etc.

En las firmas electrónicas, la firma o aceptación del firmante no es obligatoria para identificarse con la persona física. Además, fue creado bajo el control exclusivo del firmante sin ningún control sobre los equipos, certificados o sistemas utilizados.

El método de verificación de la identidad del usuario que firma a veces se realiza a través de la cuenta de correo electrónico utilizada para enviar el documento firmado. Aun así, no hay forma de saber quién firmó realmente el documento.

Firma electrónica avanzada: Las firmas electrónicas avanzadas brindan un mayor nivel de seguridad que las firmas electrónicas, logrando un equilibrio perfecto entre seguridad y facilidad de uso, al tiempo que brindan una buena experiencia de usuario y efectos legales.

La firma electrónica avanzada deberá cumplir todos los requisitos establecidos en el artículo 26 del Reglamento eIDAS:

1. Las firmas deben estar vinculadas de forma única al firmante.
2. Debido al proceso de creación de esta firma, debe permitir la identificación del firmante.
3. Al crear datos usando firmas electrónicas, las firmas pueden crearse con alta confianza bajo el control exclusivo del firmante.

4. Las firmas electrónicas avanzadas deberán estar vinculadas a los datos por ellas firmados de forma que pueda detectarse cualquier modificación posterior de los mismos.

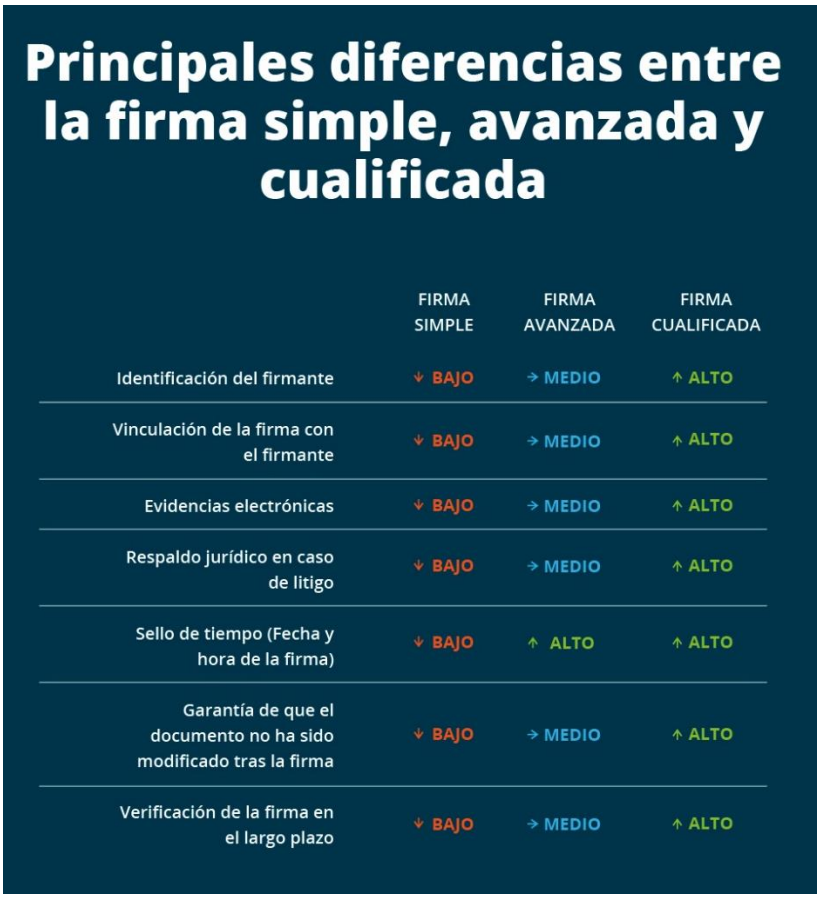
Las autoridades de los Estados miembros utilizan diferentes formatos de firma electrónica avanzada para las firmas electrónicas. No obstante, deben soportar técnicamente al menos una serie de formatos de firma electrónica avanzada a la hora de recibir documentos firmados.

Firma electrónica cualificada: Las firmas cualificadas son el tipo de firma con máxima robustez jurídica, dándonos una mayor seguridad en caso de conflictos legales. Sin embargo, esta también debe cumplir con tres requisitos básicos:

1. El firmante debe estar vinculado e identificado de forma única con la firma.
2. Los datos utilizados para crear la firma deben estar bajo el control exclusivo del firmante.
3. Debe tener la capacidad de garantizar que los datos no han sido modificados después de firmar

El certificado digital en sí mismo se denomina "certificado de firma electrónica emitido por un proveedor de servicios de confianza calificado". El certificado debe ser emitido por una autoridad certificadora, que es una entidad oficialmente reconocida que respalda la identidad del firmante.

Figura 2: *Principales diferencias entre la firma simple, avanzada y cualificada*



Fuente: https://blog.neothek.com/la-diferencia-entre-las-firmas-electronicas-y-las-firmas-digitales/

Mientras que, en el Perú, la ley nos otorga una clara definición de las firmas electrónicas y firmas digitales, ambas incluidas en la Ley 27269.

Figura 3: *Diferencias entre firma electrónica y firma digital*

Fuente: “https://lpderecho.pe/diferencias-firma-electronica-firma-digital/”

Firma Electrónica: significa cualquier símbolo basado en medios electrónicos destinada a reconocer al firmante y asociar inequívocamente al firmante de un documento. Asimismo, se ha determinado que las firmas electrónicas tienen la misma validez legal que las firmas manuscritas.

Por tanto y según lo establecido en la Ley 27269 podemos distinguir 2 tipos de firma electrónica:

Firma Electrónica Simple: Para las transacciones cotidianas

El primer tipo de firma electrónica es una firma electrónica simple. Este es el nivel más bajo de seguridad y son datos electrónicos que se adjuntan o vinculan lógicamente a otros datos electrónicos y que los usuarios utilizan para las firmas. Es legalmente vinculante y puede ser admisible como prueba en los tribunales, pero probablemente deba complementarse con otras pruebas. De hecho, una firma digital no puede identificar inequívocamente a un usuario en todos los casos en los que podría usarse. (Reader, 2022)

Por ejemplo, una firma digital es simplemente un nombre de usuario y una contraseña para acceder a un sitio web o colocar cualquier símbolo para firmar electrónicamente un archivo PDF.

Firma electrónica avanzada: Para transacciones de alto valor

Esta firma identifica claramente al firmante. Además, gracias a ello, es posible detectar si los datos firmados han sido modificados posteriormente. La creación de este tipo de firma electrónica utiliza datos generados (como datos biométricos y contraseñas de un solo uso) que están a disposición del firmante y bajo su control exclusivo, lo que otorga al firmante un alto grado de confianza. Además, se puede garantizar la integridad del contenido firmado (usando técnicas criptográficas para hacer irreversible el sello de tiempo y asociando la firma con la identidad del firmante). Las firmas electrónicas avanzadas aseguran la identidad del firmante y aportan más seguridad jurídica ya que los datos no pueden ser manipulados ni alterados posteriormente. (Reader, 2022)

Un ejemplo de firma electrónica avanzada es una firma biométrica manuscrita.

Firma Digital: Tipo de firma electrónica que utiliza criptografía simétrica y está asociada a dos claves, una clave privada y una clave pública.

La firma electrónica cualificada o firma digital es una firma generada utilizando equipos calificados para la generación de firmas digitales bajo un certificado emitido por un proveedor de servicios de autenticación. La identidad del titular del certificado (por ejemplo, si solicita un certificado digital necesita presentarse en la oficina del RENIEC para acreditar su identidad antes de la emisión del certificado). (RENIEC, 2022)

Una firma electrónica homologada o certificada tiene la misma validez legal que una firma manuscrita. Es un tipo de firma electrónica para documentos oficiales en Perú. El certificado digital contenida en el DNIe es un ejemplo de este tipo.

Figura 4: *Firma Electrónica VS Firma Digital*

Fuente: “https://kb.rolosa.com/diferencias-entre-firma-digital-y-firma-electronica/”

La seguridad digital: La seguridad de los datos es de suma importancia para cada organización e individuo. La seguridad se refiere a la protección de la información valiosa contra el acceso no autorizado y la destrucción. La seguridad de los datos es un proceso continuo que debe ser monitoreado y actualizado regularmente. Al proteger los datos, es importante tener en cuenta la naturaleza de los datos y las medidas de seguridad físicas y lógicas implementadas.

En primer lugar, los datos deben almacenarse de forma segura para evitar pérdidas y manipulaciones. Los datos confidenciales deben almacenarse en un disco duro separado o en una parte diferente del sistema informático. Además, todos los archivos deben estar encriptados para garantizar que nadie pueda leerlos sin la clave. También debe existir un plan de respaldo en caso de que haya una pérdida de datos. Se debe almacenar una copia de seguridad completa en otra unidad o medio para que se pueda restaurar en caso de que haya un problema con el dispositivo de almacenamiento principal. Todo esto garantiza que sus datos permanezcan seguros en todo momento.

A continuación, se deben implementar medidas de prevención para violaciones de datos accidentales o intencionales. Una buena planificación de la seguridad permite una recuperación rápida después de una infracción; por lo tanto, es crucial etiquetar todos los dispositivos perdidos o robados con información de

identificación. Además, debe crear un registro de todas las actividades sospechosas y contactos con su organización. De esta manera, puede informar contactos sospechosos a las fuerzas del orden público de inmediato para que puedan investigar más a fondo los incidentes. También se deben realizar auditorías periódicas para garantizar que sus medidas de seguridad estén actualizadas con las mejores prácticas actuales y los avances tecnológicos.

Finalmente, debe implementar medidas de seguridad para evitar el acceso no autorizado a sus datos. La medida más común es el cifrado: codifica todos sus datos para que nadie más que el personal autorizado pueda leerlos. Otra medida es triturar registros en papel; de esta manera, solo el personal autorizado puede acceder a sus datos y destruir los registros originales después. También puede utilizar botones de congelación en documentos importantes para evitar que se realicen copias no autorizadas y se utilicen en su contra más adelante. Todas estas estrategias garantizan que sus datos estén protegidos contra el acceso no autorizado y permiten que las personas autorizadas accedan a su información cuando sea necesario.

Los resultados de no proteger los datos pueden ser devastadores: no solo se perderá información valiosa, sino también riesgos de seguridad. no tendrá a nadie a quien informar. La protección de datos es un proceso continuo que debe ser monitoreado y actualizado periódicamente. Al proteger los datos, es importante tener en cuenta la naturaleza de los datos y las medidas de seguridad físicas y lógicas existentes. Si se produce una infracción, la implementación de medidas de prevención reducirá enormemente el tiempo de recuperación de un incidente y permitirá proteger la información valiosa.

Según (VERIDICA, 2019) la seguridad de los documentos requiere hacer un seguimiento de la autenticidad y las medidas de seguridad de cada documento de identificación. Esto incluye asegurarse de que cada uno no pueda ser alterado, falsificado o emulado.

Para lo cual identifica 3 niveles de seguridad:

Nivel 1 (Overt Features – Características Evidentes):

Este es el nivel más bajo de comprensión.

Los documentos presentan elementos de seguridad que se pueden identificar con la vista o el tacto. Algunos de estos incluyen hologramas combinados, seguridad táctil, impresión láser, tintas ópticas OVI y más. Estas características se pueden encontrar en el primer nivel de seguridad.

Nivel 2 (Covert Features – Características Encubiertas):

Un documento para ser verificado deberá pasar por herramientas simples y se fácil utilización. Algunas de las funciones de seguridad que requieren equipo especial son tinta invisible, un chip biométrico, microimpresión y más. Estas características ayudan a controlar las medidas de seguridad realizadas por profesionales capacitados.

Nivel 3 (Nivel forense):

Se necesitan laboratorios forenses especializados para analizar adecuadamente un documento a este nivel. Esto es para evitar que alguien duplique el documento o altere su contenido. Además, estos laboratorios deben mantenerse privados para proteger la identidad del propietario del documento.

Poder: El poder es un negocio jurídico unilateral, por medio del cual un sujeto confiere a otro, la facultad de representación voluntaria, para poder representarlo y ejercer determinados actos en su nombre.

En el Perú, existen tres modalidades de poder otorgados antes los Notario, siendo los siguientes: Poder por escritura Pública, Poder fuera de registro y Poder por carta con firma legalizada.

Para determinar la modalidad del poder, la Ley del Notariado, ha establecido como criterio la cuantía, conforme se detalla a continuación:

- ✓ Poder por carta con firma legalizada (hasta 0.5 de la UIT).
- ✓ Poder fuera de registro (superior al 0.5 de la UIT e inferior a 3 UIT).
- ✓ Poder por Escritura Pública (mayores a 3UIT).

De las modalidades antes mencionada, el presente trabajo, se referirá al Poder por Escritura Pública, ello en atención a que según las normas del derecho registral y al principio de titulación autentica, las inscripciones de los actos y derechos en los Registros Públicos se realizan en mérito de los instrumentos públicos.

Certificado de vigencia de poder: El certificado de vigencia de poder es una publicidad formal certificada, de tipo compendioso expedido por un abogado certificador de la SUNARP, mediante el cual se acredita la existencia del apoderamiento o representación en el Registro de Mandatos y poderes o Registro de Personas Jurídicas; a la fecha de su expedición.

Documento digital:

Cuando una persona envía un documento electrónico a otra, está confiando en que el destinatario manejará la información con cuidado. Un destinatario puede eliminar, modificar o reenviar un mensaje sin consecuencias. Sin embargo, cuando un mensaje se envía electrónicamente, es susceptible de varias formas de robo o modificación no deseada. Por lo tanto, es importante que los usuarios comprendan cómo proteger la privacidad y la seguridad de sus datos cuando transmiten mensajes electrónicamente.

Varios delitos en Internet implican el robo de información confidencial transmitida electrónicamente. Por ejemplo, un mensaje de correo electrónico puede contener la información bancaria de una persona o comunicaciones internas relacionadas con las políticas de la empresa. Dado que la mayoría de los usuarios de Internet están familiarizados con este tipo de robo como "piratería", es posible que no comprendan completamente los riesgos de seguridad asociados con los documentos electrónicos. Esencialmente, estos riesgos aumentan cuando se envía un mensaje desde una computadora u otro dispositivo electrónico que ha sido comprometido por intrusos.

Los riesgos de robo de documentos aumentan cuando las personas transmiten información personal por correo electrónico u otros medios electrónicos. Por lo general, dicha información incluye detalles bancarios, números de Seguro Social y otros datos confidenciales almacenados en archivos electrónicos. Por lo tanto, es importante que los usuarios entiendan cómo proteger la privacidad y

seguridad de sus datos cuando transmiten mensajes electrónicamente. Esto se puede hacer mediante el uso de encriptación y asegurando que solo las personas autorizadas tengan acceso a los dispositivos utilizados para transmitir mensajes.

Muchas empresas toman medidas adecuadas para salvaguardar la seguridad de sus documentos electrónicos. Emplean contraseñas estrictas para acceder a los archivos de la empresa y evitan que los empleados compartan archivos entre sí. Además, pueden configurar su software para eliminar automáticamente archivos antiguos o modificados para que las versiones antiguas de sus documentos no causen ningún problema. Sin embargo, estas medidas son tan efectivas como el nivel de seguridad establecido por el fabricante; en algunos casos, pueden no existir en absoluto. Por lo tanto, es importante que los usuarios entiendan cómo proteger la privacidad y seguridad de sus datos cuando transmiten mensajes electrónicamente.

Cada remitente debe estar familiarizado con cómo proteger la privacidad y seguridad de sus transmisiones cuando transmite mensajes electrónicamente. . Unas pocas precauciones simples contribuirán en gran medida a proteger la información confidencial del acceso no autorizado. Al mismo tiempo, quienes envían documentos electrónicos deben asegurarse de que los destinatarios sigan las pautas de seguridad pertinentes. Sin un manejo adecuado de los datos transmitidos, cualquier ventaja obtenida con el uso de un formato electrónico podría perderse debido a usos fraudulentos por parte de los destinatarios.

(Caspa Vega & Portugal Vargas, 2021) nos describe en su obra “Servicio para la generación de firma digital y autenticación electrónica usando los certificados digitales contenidos en el DNI electrónico” que buscando desarrollar un servicio que permitiera la generación de firmas digitales de documentos PDF, dándoles el mismo valor legal que las firmas manuscritas, y la autenticación electrónica para el acceso a aplicaciones web.

El servicio permitirá adecuar el uso de los certificados digitales incluidos en el DNI electrónico peruano a la normativa legal vigente y podrá integrarse de forma fácil, rápida y sencilla en cualquier aplicación web existente o nueva.

Para lograr los objetivos anteriores, se implementará un servicio de generación de firmas digitales según lo especificado en los Lineamientos para la Certificación de Aplicaciones de Software del INDECOPI, que especifican los requisitos funcionales que deben cumplir las aplicaciones de software de clave pública. con DNI electrónico.

Parte de estos requisitos también se implantarán en los servicios de certificación electrónica, lo que garantizará que el servicio cumple los requisitos necesarios para las operaciones de firma digital y certificación electrónica mediante certificados digitales contenidos en tarjetas de identificación electrónicas.

La implementación de la solución propuesta incluirá el desarrollo de una aplicación de PC para ejecutar en la computadora y el desarrollo de una aplicación web para ejecutar en la computadora.

Se conectarán a estas aplicaciones de PC y también habrá una aplicación web de mantenimiento para gestionar la autorización de uso del servicio.

Por ello, (Espinoza, 2018) nos indica en su obra titulada: “Entre la firma electrónica y la firma digital: aproximaciones sobre su regulación en el Perú” que las operaciones electrónicas suelen desarrollarse en entornos inseguros, por lo que requieren de ciertos mecanismos técnicos para identificar al firmante y hacer reconocer la voluntad expresada en un medio seguro con legitimidad. En ese sentido, este relevamiento pretende determinar cuáles son los aspectos normativos que permiten el uso de firmas electrónicas y digitales en el Perú; en ese sentido, también busca comprender el entorno en el que el derecho informático puede reconocer legalmente las tecnologías antes mencionadas.

(Jara Díaz, 2005) con su trabajo titulado “Modelo de un sistema integrado para el proceso de verificación de firmas” resuelve el problema del manejo de la información en el menor tiempo posible, y por ende se emiten los reportes a tiempo, para lo cual se desarrolla un modelo del Sistema Integrado de Verificación de Firma RENIEC, ya que solo así se pueden recibir los módulos y los reportes requeridos en la institución En, se pueden utilizar los módulos existentes de procesos que suelen trabajar directamente, como la verificación electrónica y la verificación semiautomática. El RENIEC es un organismo constitucional autónomo, integrado en el sistema electoral, con personería

jurídica de derecho público interno y con facultades registrales, técnicas, administrativas, económicas y financieras. La Subdirección de Actividades Electorales es un órgano de apoyo de la Jefatura Estatal que coordina la actualización de los padrones electorales y verifica o verifica la autenticidad de las firmas de las listas de simpatizantes presentadas por las organizaciones de la sociedad civil en las elecciones en los casos previstos por la ley. Coordina la actualización del padrón electoral con la Subjefatura Estatal y Gerencia de Tecnologías de la Información. Por lo tanto, la subadministración de campañas electorales necesita de un sistema integrado de verificación de firmas para poder atender mejor a los ciudadanos, es por ello que el modelado del sistema de desarrollo utilizando UML Unified Modeling Language, utilizando el problema de diagrama más importante requiere del conocimiento de la solución. comprensión. A su vez, actualmente se cuenta con un sistema de verificación electrónica y un sistema de verificación de firma semiautomático, los cuales se encuentran integrados, y se ha desarrollado un prototipo receptor en la misma subdirección de campaña electoral, elaborado de acuerdo a las necesidades del distrito. Además, no se han incorporado módulos de programación, que es una necesidad de la región. La subdirección de campañas electorales cuenta con un sistema que aún no está integrado, y con esta propuesta pretendemos incorporar el prototipo receptor al sistema integral de verificación de firmas que actualmente opera en la región.

(Arriola Pareja & Lucana Del Castillo, 2021) en su estudio titulado “Archivo registral digital como un medio de seguridad jurídica en el Perú” examina el expediente registral, el almacenamiento y conservación de sus documentos así como la seguridad comercial. También examinamos la legislación vigente en nuestro país sobre archivos registrales y cómo beneficia el tráfico comercial. Luego analizamos los resultados que logramos, que nos llevaron a crear documentos de registro digitales. Para proponer un sistema de registro digital, utilizamos un enfoque legal, dogmático y cualitativo. Nuestro análisis involucra entrevistas con expertos y revisión de literatura relevante. Este enfoque combinado nos proporciona un análisis interpretativo y descriptivo que también propone un marco para la creación de documentos de registro.

(Coronel García, 2020) En su trabajo titulado “Implementación de los documentos notariales electrónicos en el Perú para mejorar la seguridad jurídica” tiene como objetivo encontrar nuevas formas de aumentar la seguridad jurídica a través de documentos notariales electrónicos. Hacerlo se utilizaría como objetivo y se probaría la legalización de los documentos notariales electrónicos como criterio para implementarlos. Sus principios de protección y publicidad la legitiman. Un proyecto paralelo no relacionado tiene como objetivo analizar el daño causado al sistema legal en Perú debido a la falta actual de documentos notariales electrónicos en el país. Luego, este proyecto sugiere formas de modificar las leyes para resolver este problema. La modernización de la tecnología notarial y la mejora de la seguridad de los documentos notariales están a la vanguardia de este proyecto. Las entrevistas con expertos notarios llevaron a una mejor comprensión de los efectos que tiene su trabajo en la notarización electrónica. Otras entrevistas se centraron en examinar la necesidad de certeza de los sistemas legales modernos y cómo se relaciona con la modernización de la tecnología notarial. Estas entrevistas dieron lugar a recomendaciones de cambios en el sistema notarial. La hipótesis plantea que los documentos notariales electrónicos aumentan la seguridad jurídica en el Perú. Al hacer una contribución tan grande a la seguridad jurídica, esta hipótesis resulta extremadamente positiva. También muestra que la política del país fomenta la modernización del sistema de gestión administrativa del país a través de la notarización electrónica. Estos dos hechos complementan el poder de los documentos notariales como fundamento de los procesos judiciales peruanos.

(Franco Ccallo, 2018) en su investigación titulada “Sistema web basado en tecnología PKI, para mejorar la seguridad de la gestión documental en la 32ª Brigada de Infantería – 2018” tiene como objetivo determinar formas de aumentar la seguridad jurídica mediante la implementación de documentos notariales electrónicos. También busca examinar métodos para incorporar estos documentos al sistema judicial, así como métodos para utilizar tecnologías electrónicas en procesos notariales. Este estudio analiza los criterios para la legalización de documentos y evalúa los cambios necesarios en la legislación actual. Además, examina el daño actual del Perú a la seguridad jurídica junto con la legislación internacional que implementó los documentos notariales

electrónicos. Finalmente, este estudio propone crear una nueva legislación basada en sus hallazgos. Se fomenta la modernización y mejora de la seguridad de los documentos notariales a través de debates sobre el papel del notario y sus efectos en la notarización electrónica. Se realizaron entrevistas adicionales sobre el tema para discutir cómo afecta la notarización electrónica y la modernización de cómo se hace la tecnología notarial. Se analizó la importancia de la seguridad jurídica para la modernización de la tecnología notarial y se recomendaron cambios. Finalmente, se discutieron leyes nuevas o revisadas junto con un análisis técnico/legal. Para establecer la seguridad jurídica de los documentos notariales, esta hipótesis muestra que la implementación de notarizaciones electrónicas mejora el sistema legal del país de Perú. Esto se traduce en una importante contribución a la seguridad jurídica de los documentos notariales, que son la piedra angular de su actividad. También muestra que la modernización con modernos sistemas de gestión administrativa es parte de la política de modernización del país.

(TACO ARIAS & GAMARRA RAMIREZ, 2005) nos dice que muchas personas utilizan documentos digitales todos los días sin tener en cuenta su seguridad. Debido a que los documentos digitales son públicos y se usan con frecuencia, muchas personas no consideran su seguridad. Una de las razones de esto es que no se ha creado un software como este para verificar la autenticidad de un documento. Sin este software, las personas pueden recibir documentos con funciones de seguridad rotas. Por ejemplo, es posible que un destinatario no pueda leer archivos con cifrado roto porque el creador no creó el archivo con una clave de cifrado. Se puede acceder a este software a través de Internet para que los destinatarios no tengan que preocuparse por las funciones de seguridad rotas en los documentos enviados.

Los documentos electrónicos deben mantener la confidencialidad, la integridad y el hecho de que fueron escritos por un autor específico. Esto se logra mediante el uso de técnicas criptográficas que se estudian y utilizan comúnmente. Una de ellas es la criptografía asimétrica, que mencionamos en el texto.

Los avances tecnológicos, como el protocolo SSL para la transmisión segura de datos y las firmas digitales, surgieron gracias a su creación.

Bajo nuestro sistema, los usuarios pueden compartir observaciones de documentos con sus contactos a través de SSL y firmas digitales a través de una plataforma web. Además, los usuarios pueden cargar archivos para que otros los inspeccionen y firmen. Esto se hace a través de nuestra plataforma web propuesta.

Para mantener el sistema y facilitar la actualización, lo construimos con una arquitectura en capas basada en componentes. Además, nuestro informe documenta el proceso de desarrollo y lo superpone para que podamos reutilizar el sistema fácilmente.

III. METODOLOGÍA

3.1. Tipo y diseño de investigación

3.1.1. Tipo de Investigación

La investigación actual cae en la categoría básica de niveles descriptivos correlacionales. Este tipo de investigación se utiliza para mejorar y/o comprender un problema particular que es objeto de investigación. El autor realizará un tipo de investigación básica y utilizarán un diseño no experimental transversal exploratorio descriptivo, es decir, un estudio en el que no se manipula intencionalmente la variable independiente para evaluar su efecto sobre la variable dependiente; las observaciones solo pueden ser hecho en su entorno natural. (Hérnandez Sampieri, Fernandez Colado, & Baptista Lucio, 2014)

3.1.2. Diseño de investigación

Se seguirá un diseño de investigación descriptivo correlacional puesto que se describirá el problema y se analizará la relación de las variables seguridad digital (Principal) y firma electrónica (secundaria). También se sigue el diseño cuantitativo, debido a que los resultados del análisis de los certificados de vigencia de poder emitidos por la Oficina Registral de Andahuaylas en el año 2022 serán cuantificados; y por último seguiremos el diseño retrospectivo trasversal puesto que analizaremos los certificados de vigencia de poder emitidos por la Oficina Registral de Andahuaylas durante el año 2022 solo al momento del presente estudio.

3.2. Población y muestra

3.2.1. Población:

El presente trabajo de investigación se aplicará a los certificados de vigencia de poder emitidos por la Oficina Registral de Andahuaylas en el 2022, por lo que la población serán los 1855 certificados de vigencia de poder emitidos por la Oficina Registral de Andahuaylas de la Súper Intendencia Nacional de los Registros Públicos (SUNARP) en lo que va del 2022. Para determinar el tipo de firma electrónica utilizada y el nivel de seguridad de los documentos emitidos por dicha área.

N = 1,855 certificados de vigencia de poder emitidos por la Oficina Registral de Andahuaylas de la Súper Intendencia Nacional de los Registros Públicos.

3.2.2. Muestra:

Para calcular la muestra seguiremos el modelo matemático descrito en el “Anexo 8”; en donde se analiza un modelo probabilístico simple y se obtiene como resultado n = 70.26 Certificados de vigencia de poder.

Por ello se tomará como muestra:

n = 70 certificados de vigencia de poder emitidos por la Oficina Registral de Andahuaylas de la Súper Intendencia Nacional de los Registros Públicos.

3.3. Técnicas e instrumentos de recolección de Datos

La técnica por utilizar en el presente estudio será la del levantamiento de información de los certificados de vigencia de poder emitidos por la Oficina Registral de Andahuaylas los cuales serán cuantificados según el escalamiento de Likert. El instrumento que se utilizará será la guía de verificación tanto para la variable principal (Seguridad digital) y la variable secundaria (Firma electrónica).

3.4. Procedimientos

Teniendo definido el diseño metodológico y los objetivos para la presente investigación se procederá de la siguiente manera:

La técnica para recolección de datos se realizará a través del levantamiento de información de los diferentes certificados de vigencia de poder emitidos por el área de publicidad registral de la oficina registral de Andahuaylas.

Para cuantificar los valores obtenidos el levantamiento de información se utilizará una tabla de valores comparativos.

Una vez cuantificados los resultados estos se procesarán a través del programa informático SPSS para responder los diferentes criterios de la presente investigación.

Por último, se interpretarán y describirán los resultados obtenidos.

3.5. Métodos de análisis de datos

Para el análisis de datos se utilizará el paquete estadístico SPSS y para determinar la aceptación o rechazo de la hipótesis utilizaremos la prueba no paramétrica “RHO de Spearman”, la cual es una prueba no paramétrica de correlación lineal.

3.6. Aspectos éticos

Garantizar una buena práctica de investigación significa, como investigador, asumir que la investigación no le hará ningún daño ni afectará negativamente a otros.

Para que lo anterior funcione, los principios son los siguientes:

1. Sujeto a la política de confidencialidad y protección de datos, toda la información utilizada en la encuesta se mantendrá confidencial.
2. En lo que respecta a las reservas, recogida y análisis de datos, se atenderán las solicitudes de información específica y suficiente. Cuando la fuente sea directamente una persona física, se obtendrá autorización previa.
3. No hay diferencia y sinergia, y todas las fuentes se refieren a recursos humanos, lo cual es consistente con la particularidad de la muestra de investigación.
4. Se aprueba el estudio y todos los RR.HH. involucrados en la encuesta entienden los objetivos y brindan información clara.
5. Sujeto a la propiedad de la investigación y/o autoría de los resultados.

IV. RESULTADOS

4.1. Objetivo General: Como objetivo principal para el presente estudio se planteó “Determinar la relación que existe entre la Seguridad digital y la Firma electrónica utilizada en los certificados de vigencia de poder emitidos por la Oficina Registral de Andahuaylas”; por lo que una vez obtenido los resultados de los análisis para ambas variables (seguridad digital y firma electrónica) se pasó a realizar la prueba de normalidad.

Prueba de normalidad

Definamos:

H_0: La muestra sigue una distribución normal (Sig. > 0.05).

H_1: La muestra no sigue una distribución normal (Sig. <= 0.05).

Tabla 1: *Prueba de normalidad*

Pruebas de normalidad						
	Kolmogorov-Smirnov[a]			Shapiro-Wilk		
	Estadístico	Gl	Sig.	Estadístico	gl	Sig.
Seguridad digital	0.263	70	0	0.870	70	0
Firma electrónica	0.268	70	0	0.803	70	0
a. Corrección de significación de Lilliefors						

Fuente: Elaboración propia (Cálculo par prueba de normalidad SPSS).

En las muestras se analizará el nivel de significancia (Sig.) para las dos variables (Seguridad digital y Firma electrónica), al ser una muestra mayor a 50 tomaremos en cuenta únicamente la prueba de normalidad de “Kolmogorov-Smirnov”.

Como se puede apreciar el nivel de significancia es 0.0; por tanto, nuestra muestra no sigue una distribución normal y para poder determinar la correlación de nuestras variables deberemos utilizar la prueba estadística “Rho de Spearman”

Cálculo del coeficiente de correlación de Spearman

$$\rho = 1 - \frac{6\sum d^2}{n(n^2-1)}$$

Dónde:

ρ : Coeficiente de correlación de Spearman.

d : Diferencia entre los correspondientes datos en orden x – y.

n : Numero de pareja de datos.

Remplazando:

$$\rho = 0{,}91701$$

Realizando el cálculo en SPSS

Tabla 2: *Correlación de Rho de Spearman*

Correlaciones				
			Seguridad Digital	**Firma Electrónica**
Rho de Spearman	**Seguridad digital**	Coeficiente de correlación	1	0.917
		Sig. (bilateral)	0	0
		N	70	70
	Firma electrónica	Coeficiente de correlación	0.917	1
		Sig. (bilateral)	0	0
		N	70	70

Fuente: Elaboración propia (Resultado del cálculo SPSS)

De la tabla 10 presentada en el anexo 7 “Grado de relación según coeficiente de correlación” podemos indicar que las variables “Seguridad digital” y “Firma electrónica” **tienen una correlación positiva perfecta**, puesto que el coeficiente de correlación de Spearman es de 0.91701.

4.1. Objetivo específico 1: Como objetivo específico 1 se determinó “Identificar el nivel de Seguridad digital en los certificados de vigencia de poder emitidos por la Oficina Registral de Andahuaylas” para lo cual se establece la siguiente tabla:

Tabla 3: *Definición de VERIDICA VS Niveles de seguridad digital*

Nivel de Seguridad	Rango	Resultado
Alto	[26 a 45]	0 (0%)
Medio	[16 a 25]	63 (90%)
Bajo	[0 a 15]	7 (10%)

Fuente: Contrastación de resultado con (VERIDICA, 2019).

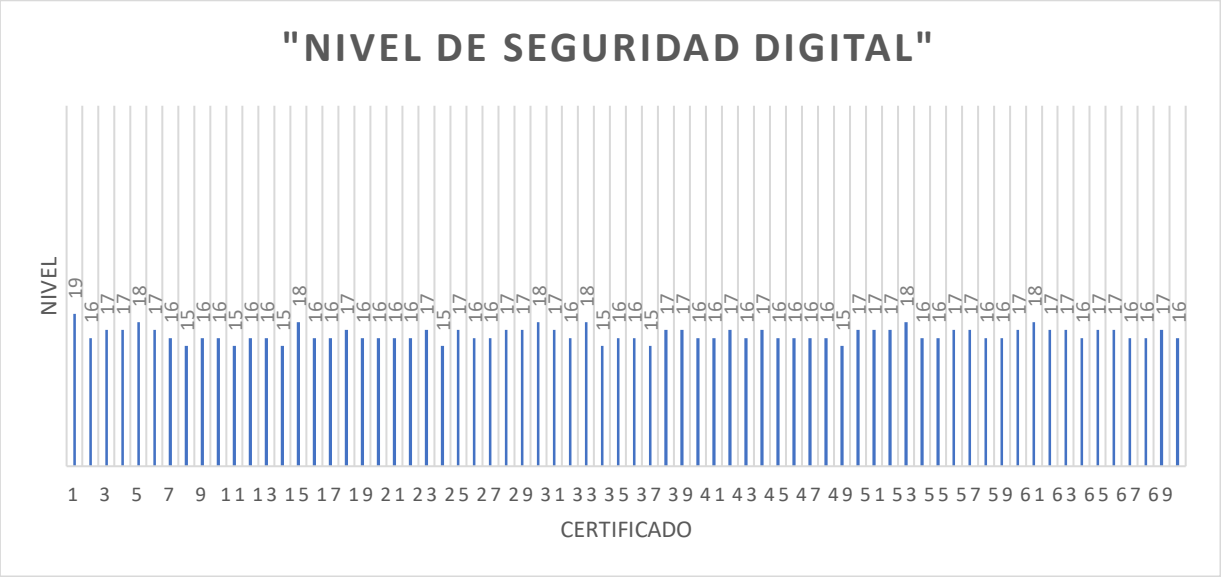
Según lo definido por (VERIDICA, 2019) nos estable 3 nivel de seguridad para los documentos los cuales son:

- Nivel 1 (Overt Features – Características Evidentes) – Alto.
- Nivel 2 (Covert Features – Características Encubiertas) – Medio.
- Nivel 3 (Nivel forense) – Bajo.

De los cuales el 0 % de los certificados de vigencia de poder emitidos por la Oficina Registral de Andahuaylas obtiene el nivel de seguridad “Alto”; También se aprecia que un 90 % de los certificados presentan un nivel “Medio” y por ultimo el 10 % de los certificados presenta un nivel “Bajo”.

Tomamos la definición de los niveles establecidos por (VERIDICA, 2019); y analizamos los resultados para la variable seguridad digital:

Figura 5: *Cuantificación de la variable seguridad digital*



Fuente: Elaboración propia (cuantificación de variables)

Como se puede apreciar y al cuantificar la variable “Seguridad digital” esta obtiene una puntuación que va de un máximo de 19 hasta un mínimo de 15 puntos obtenidos lo cual nos indica que va desde un nivel bajo a medio en la escala definida por VERIDICA (2019).

4.2. Objetivo específico 2: Como segundo objetivo se tiene el “Identificar el nivel o tipo de Firma electrónica utilizado en los certificados de vigencia de poder emitidos por la Oficina Registral de Andahuaylas”; para determinar esto se estableció la siguiente tabla.

Tabla 4: *Cuantificación del tipo de firma electrónica VS Niveles de firma electrónica.*

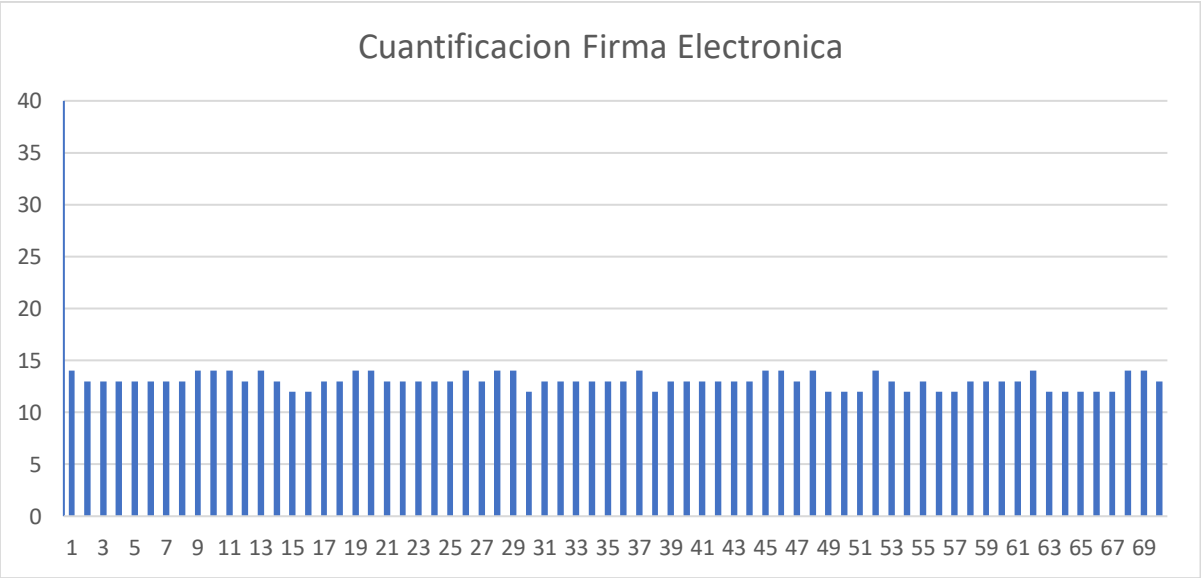
Tipo de firma electrónica	Rango	Resultado
Avanzado	[21 a 40]	0 (0%)
Simple	[16 a 20]	70 (100%)

Fuente: (elDAS, 2014)

Tomaremos la definición y categorización definida por el (elDAS, 2014), y cuantificaremos la variable “firma electrónica”.

De la cual se aprecia que el 100% de los certificados emitidos por la Oficina Registral de Andahuaylas utiliza el tipo de firma electrónica “Simple”.

Figura 6: *cuantificación de la variable firma electrónica.*



Fuente: Elaboración propia (resultados de análisis de variable firma electrónica).

Al cuantificar la variable “firma electrónica” se observa que esta tiene como resultado un puntaje máximo de 14 puntos y un mínimo de 12 puntos, lo cual nos indica que la firma electrónica utilizada para la emisión de certificados de vigencia de poder por la Oficina Registral de Andahuaylas es únicamente de tipo “Simple”.

V. DISCUSIÓN

Al adentrarnos en la seguridad digital de los documentos de certificado de vigencia de poder emitidos por la oficina Registral de Andahuaylas deberemos analizar la investigación de (Caspa Vega & Portugal Vargas, 2021) titulada “Servicio para la generación de firma digital y autenticación electrónica usando los certificados digitales contenidos en el DNI electrónico” en la cual logro desarrollar un aplicativo de escritorio y web para poder generar documentos en PDF incrustando el certificado contenido en el Documento Nacional de Identidad electrónico DNIe; En esta investigación no se logra otra cosa que la firma digital o firma electrónica cualificada puesto que protege el documento en cuestión a través del cifrado y la incrustación de un certificado digital, en este caso es uno emitido por el “Registro Nacional de Identificación y estado Civil” RENIEC, por lo que se puede indicar que este documento es altamente seguro.

También al analizar la investigación de (Espinoza, 2018) titulada “Entre la firma electrónica y la firma digital: aproximaciones sobre su regulación en el Perú” nos indica que las operaciones electrónicas se suelen desarrollar en entornos bastante inseguros por lo que es muy necesario identificar plenamente al firmante para asi reconocer su voluntad al expresar o firmar un determinado documento; por lo que en estos casos es muy necesario el uso de una firma electrónica avanzada o mejor aún la utilización de la firma digital o firma electrónica cualificada par que de esta manera se tenga una plena identificación del firmante y el documento resultado de este proceso esté completamente seguro y cifrado.

Luego (Jara Díaz, 2005) en su artículo titulado “Modelo de un sistema integrado para el proceso de verificación de firmas” resuelve el problema para el majo de información en el menor tiempo posible puesto que la aplicación sugerida en este artículo suele corroborar con RENIEC la validez del certificado incluido en los documentos recepciónados por el mismo; en este punto es importante indicar que a la fecha los certificados para la firma digital o firma electrónica cualificada son emitidos por diversas empresas alrededor del mundo y solo hacer la verificación en RENIEC no sería suficiente para determinar la validez de estos documentos por lo que en la actualidad el aplicativo Adobe Reader que está disponible de manera gratuita nos ayuda a realizar la verificación de los

certificados contenidos en los documentos que abramos en esta app asi como también nos brinda la opción de firmar documentos mediante un certificado emitido por una empresa autorizada.

Mientras que (Arriola Pareja & Lucana Del Castillo, 2021) en su artículo titulado “Archivo registral digital como un medio de seguridad jurídica en el Perú” nos muestra las bondades de tener un archivo completamente digital y altamente seguro basándose en las normas y leyes vigentes en el Perú. De lo cual, y con todo lo acontecido en diciembre del 2022 es muy recomendable tener los archivos digitalizados y de un modo que estos permanezcan intangibles en el tiempo, tengan una alta disponibilidad y reglas muy claras para su accesibilidad por lo que una vez más caemos en el campo del uso de las firmas digitales o firmas electrónicas cualificadas para proteger los documentos digitales.

También (Coronel García, 2020) en su investigación “Implementación de los documentos notariales electrónicos en el Perú para mejorar la seguridad jurídica” busca encontrar nuevas formas para aumentar la seguridad jurídica a través de documentos notariales electrónicos, utilizando firmas electrónicas que garanticen la intangibilidad y alta disponibilidad de los documentos emitidos por Notarios Públicos, al contrastar los resultados este logro alcanzar niveles óptimos de seguridad digital en los documentos electrónicos firmados por Notarios Públicos a través de la utilización de firmas digitales.

Por otro lado (Franco Ccallo, 2018), busca garantizar la intangibilidad de los documentos digitales en su investigación titulada: “Sistema web basado en tecnología PKI, para mejorar la seguridad de la gestión documental en la 32ª Brigada de Infantería – 2018” a través del uso de un conjunto de claves KPI que no es otra cosa que la utilización de firma digital o firma electrónica cualificada, logrando asi mantener seguros e intangibles los documentos electrónicos a lo largo del tiempo para su adecuado almacenamiento.

Por último (TACO ARIAS & GAMARRA RAMIREZ, 2005), nos indica que en el día a día las personas suelen utilizar documentos digitales sin importarles la seguridad de los mismos y sin ser conscientes de las consecuencias, por lo que recomienda utilizar criptografía para mantener estos documentos intangibles en el tiempo, pero esto no es mas que uno de los recursos o bondades que nos brinda la utilización de firmas digitales en nuestros documentos electrónicos.

Por todo lo antes descrito en la presente investigación se busca analizar y determinar que la seguridad digital de los documentos digitales esta correlacionada directamente con el tipo de firma utilizado para validar el mismo.

VI. CONCLUSIONES

Al analizar la variable “Seguridad Digital” en los Certificados de Vigencia de Poder emitidos por la Oficina Registral de Andahuaylas esta logra obtener una puntuación media de 16.4571 en una escala de 0 a 45 puntos posibles por lo que se concluye que el nivel de seguridad de los Certificados de Vigencia de Poder emitidos por la Oficina Registral de Andahuaylas es de un nivel Medio.

Luego se analizó la variable “Firma electrónica” en los Certificados de Vigencia de Poder emitidos por la Oficina Registral de Andahuaylas logrando un puntaje promedio de 13.0428 puntos de 40 posibles por lo que se concluye que el tipo de firma electrónica utilizada para firmara los Certificados de Vigencia de Poder en la Oficina Registral de Andahuaylas es de tipo Simple.

Por último, al analizar la correlación de las variables “Seguridad Digital” y “Firma electrónica” se concluye que ambas tienen una **“correlación positiva perfecta ($\boldsymbol{\rho = 0,91701}$)”** dado que si aumenta la puntuación del tipo de firma electrónica utilizada en los Certificados de Vigencia de Poder emitidos por la Oficina Registral de Andahuaylas también aumentara directamente la puntuación de la variable “Seguridad Digital”.

VII. RECOMENDACIONES

Se recomienda fortalecer el nivel de seguridad de los Certificados de Vigencia de Poder emitidos por la Oficina Registral de Andahuaylas puesto que al tratarse de un documento de suma importancia tanto para el ámbito comercial como personal este requiere que pueda ser validado fácilmente y también se mantenga intangible durante el periodo de su valides.

En cuanto al tipo de firma electrónica utilizado se recomienda migrar a la utilización de firmas digitales puesto que estas son muy fáciles de validar y garantizan la intangibilidad del documento.

Por último, al advertirse que la seguridad digital de los documentos de Certificados de Vigencia de Poder emitidos por la Oficina Registral de Andahuaylas depende directamente del tipo de firma utilizada para su emisión se recomienda la migración total y de forma urgente para evitar cualquier tipo de fraude a través de este documento.

REFERENCIAS

Arriola Pareja, I. L., & Lucana Del Castillo, A. L. (2021). *Archivo registral digital como un medio de seguridad jurídica en el Perú.* Cusco.

Caspa Vega, J. C., & Portugal Vargas, P. C. (2021). *Servicio para la generación de firma digital y autenticación electrónica usando los certificados digitales contenidos en el DNI electrónico.* Lima.

Congreso, C. D. (1993). *CONSTITUCIÓN POLÍTICA DEL PERÚ 1993.*

Coronel García, A. Y. (2020). *Implementación de los documentos notariales electrónicos en el Perú para mejorar la seguridad jurídica.* Lambayeque.

e-certchile. (20 de Octubre de 2020). *e-certchile*. Obtenido de https://www.e-certchile.cl/noticias/la-historia-de-la-firma-electronica-en-el-mundo

elDAS. (2014). REGLAMENTO (UE) N o 910/2014 DEL PARLAMENTO EUROPEO Y DEL CONSEJO.

Espinoza, J. F. (2018). Entre la firma electrónica y la firma digital: aproximaciones sobre su regulación en el Perú. 26.

Franco Ccallo, K. R. (2018). *Sistema web basado en tecnología PKI, para mejorar la seguridad de la gestión documental en la 32ª Brigada de Infantería – 2018.* Trujillo.

Hérnandez Sampieri, R., Fernandez Colado, C., & Baptista Lucio, M. d. (2014). *Metodologia de Investigacion.* Sabta Fe: Mc Graw Hill Education.

Jara Díaz, C. M. (2005). *Modelo de un sistema integrado para el proceso de verificación de firmas.* Lima.

LlamaPE. (19 de Octubre de 2022). *Llama PE*. Obtenido de https://llama.pe/la-historia-de-la-certificacion-digital

MINJUSDH. (2000). Ley de firmas y certificados digitales. *El Peruano*, págs. 187067-187068.

Reader, A. A. (20 de 11 de 2022). *Adobe Acrobat Reader*. Obtenido de https://www.adobe.com/la/sign/electronic-signatures.html

RENIEC. (20 de 11 de 2022). *Guía para realizar la firma digital*. Obtenido de https://www.gob.pe/institucion/reniec/campa%C3%B1as/7245-guia-para-realizar-la-firma-digital

SIGNE. (2021). *Niveles de seguridad de un documento, clasificación de técnicas y funcionalidades para su verificación o validación.* Madrid: SIGNE.

SUNARP, S. I. (29 de Mayo de 2020). RESOLUCIÓN DEL SUPERINTENDENTE NACIONAL DE LOS REGISTROS PÚBLICOS N° 058 -2020-SUNARP/SN. Lima, Peru.

TACO ARIAS, L. A., & GAMARRA RAMIREZ, S. E. (2005). *SISTEMA WEB PARA EL INTERCAMBIO SEGURO DE DOCUMENTOS ELECTRÓNICOS, UTILIZANDO FIRMAS Y CERTIFICADOS DIGITALES X509, SOBRE UN CANAL SSL.* Arequipa.

VERIDICA. (2019). niveles de seguridad en un documento. 124-130.

ANEXOS

Anexo 01 – Matriz de Consistencia

Tabla 5: *Matriz de consistencia*

PROBLEMAS	OBJETIVOS	HIPÓTESIS	VARIABLES
Problema general	**Objetivo general**	**Hipótesis general**	**Variable A**
¿Qué relación que existe entre la seguridad digital y la Firma electrónica utilizada en los certificados de vigencia de poder emitidos por la Oficina Registral de Andahuaylas?	Determinar la relación que existe entre la Seguridad digital y la Firma electrónica utilizada en los certificados de vigencia de poder emitidos por la Oficina Registral de Andahuaylas.	Existe relación significativa entre la Seguridad digital y la Firma electrónica utilizada en los certificados de vigencia de poder emitidos por la Oficina Registral de Andahuaylas.	La seguridad digital - Alta - Media - Baja

Problemas específicos	Objetivos específicos	Hipótesis específicas	Variable B
1) ¿Cuál es el nivel de Seguridad digital A en los certificados de vigencia de poder emitidos por el área de publicidad registral de la Oficina Registral de Andahuaylas? 2) ¿Cuál es el tipo de Firma electrónica B utilizada en los certificados de vigencia de poder emitidos por el área de publicidad registral de la Oficina Registral de Andahuaylas?	1) Identificar el nivel de Seguridad digital A en los certificados de vigencia de poder emitidos por el área de publicidad registral de la Oficina Registral de Andahuaylas. 2) Identificar el tipo de Firma electrónica B utilizada en los certificados de vigencia de poder emitidos por la Oficina Registral de Andahuaylas.		Firma electrónica. - Simple - Avanzada

Fuente: Elaboración propia

Anexo 02 - Ficha de investigación Seguridad digital

Nivel 1 (Overt Features – Características Evidentes)

1. ¿a simple vista es posible determinar los mecanismos de seguridad con los que cuenta el documento?
   ( ) Totalmente de acuerdo (5)
   ( ) De acuerdo (4)
   ( ) Indeciso, ni de acuerdo ni en desacuerdo (3)
   ( ) En desacuerdo (2)
   ( ) Totalmente en desacuerdo (1)

2. ¿No es necesario la utilización de ningún tipo de instrumento para su plena identificación?
   ( ) Totalmente de acuerdo (5)
   ( ) De acuerdo (4)
   ( ) Indeciso, ni de acuerdo ni en desacuerdo (3)
   ( ) En desacuerdo (2)
   ( ) Totalmente en desacuerdo (1)

3. ¿El documento se mantiene seguro a través de algoritmos de encriptación de datos?
   ( ) Totalmente de acuerdo (5)
   ( ) De acuerdo (4)
   ( ) Indeciso, ni de acuerdo ni en desacuerdo (3)
   ( ) En desacuerdo (2)
   ( ) Totalmente en desacuerdo (1)

Nivel 2 (Covert Features – Características Eencubiertas)

4. ¿mediante el uso de herramientas sencillas y de fácil acceso se puede identificar el nivel de seguridad del documento?
   ( ) Totalmente de acuerdo (5)
   ( ) De acuerdo (4)
   ( ) Indeciso, ni de acuerdo ni en desacuerdo (3)
   ( ) En desacuerdo (2)
   ( ) Totalmente en desacuerdo (1)

5. ¿Las medidas de seguridad se pueden identificar a simple vista?
   ( ) Totalmente de acuerdo (5)
   ( ) De acuerdo (4)
   ( ) Indeciso, ni de acuerdo ni en desacuerdo (3)
   ( ) En desacuerdo (2)
   ( ) Totalmente en desacuerdo (1)

Nivel 3 (Nivel forense)

6. ¿No se requieren de herramientas sofisticadas para determinar la valides del documento?
   ( ) Totalmente de acuerdo (5)
   ( ) De acuerdo (4)
   ( ) Indeciso, ni de acuerdo ni en desacuerdo (3)
   ( ) En desacuerdo (2)
   ( ) Totalmente en desacuerdo (1)

7. ¿Es posible determinar si el documento fue adulterado?
   ( ) Totalmente de acuerdo (5)
   ( ) De acuerdo (4)
   ( ) Indeciso, ni de acuerdo ni en desacuerdo (3)
   ( ) En desacuerdo (2)
   ( ) Totalmente en desacuerdo (1)

8. ¿Es posible identificar plenamente al autor del documento?
   ( ) Totalmente de acuerdo (5)
   ( ) De acuerdo (4)
   ( ) Indeciso, ni de acuerdo ni en desacuerdo (3)
   ( ) En desacuerdo (2)
   ( ) Totalmente en desacuerdo (1)

Anexo 03 - Ficha de investigación Firma electrónica

Firma electrónica simple

1. ¿El documento contiene sello de tiempo (Fecha y hora) en la que fue firmado?
   ( ) Totalmente de acuerdo (5)
   ( ) De acuerdo (4)
   ( ) Indeciso, ni de acuerdo ni en desacuerdo (3)
   ( ) En desacuerdo (2)
   ( ) Totalmente en desacuerdo (1)

2. ¿El firmante es identificado plenamente?
   ( ) Totalmente de acuerdo (5)
   ( ) De acuerdo (4)
   ( ) Indeciso, ni de acuerdo ni en desacuerdo (3)
   ( ) En desacuerdo (2)
   ( ) Totalmente en desacuerdo (1)

3. ¿La firma está vinculada únicamente con el firmante?
   ( ) Totalmente de acuerdo (5)
   ( ) De acuerdo (4)
   ( ) Indeciso, ni de acuerdo ni en desacuerdo (3)
   ( ) En desacuerdo (2)
   ( ) Totalmente en desacuerdo (1)

Firma electrónica avanzada

4. ¿Los datos utilizados para la creación de la firma se encuentran bajo el control exclusivo del firmante?
   ( ) Totalmente de acuerdo (5)
   ( ) De acuerdo (4)
   ( ) Indeciso, ni de acuerdo ni en desacuerdo (3)
   ( ) En desacuerdo (2)
   ( ) Totalmente en desacuerdo (1)

5. ¿El documento firmado guarda evidencias electrónicas? (Modificaciones, versiones, etc.)
   ( ) Totalmente de acuerdo (5)
   ( ) De acuerdo (4)
   ( ) Indeciso, ni de acuerdo ni en desacuerdo (3)
   ( ) En desacuerdo (2)
   ( ) Totalmente en desacuerdo (1)

6. ¿El documento firmado cuenta con respaldo jurídico en caso de litigio?
   ( ) Totalmente de acuerdo (5)
   ( ) De acuerdo (4)
   ( ) Indeciso, ni de acuerdo ni en desacuerdo (3)
   ( ) En desacuerdo (2)
   ( ) Totalmente en desacuerdo (1)

7. ¿El documento es intangible luego de la firma?
   ( ) Totalmente de acuerdo (5)
   ( ) De acuerdo (4)
   ( ) Indeciso, ni de acuerdo ni en desacuerdo (3)
   ( ) En desacuerdo (2)
   ( ) Totalmente en desacuerdo (1)

8. ¿Es posible determinar la veracidad y la validez de la firma en un largo plazo?

( ) Totalmente de acuerdo (5)

( ) De acuerdo (4)

( ) Indeciso, ni de acuerdo ni en desacuerdo (3)

( ) En desacuerdo (2)

( ) Totalmente en desacuerdo (1)

Anexo 04 - Tabla de operacionalización de variables

Tabla 6: *Operacionalizacion de variables*

Variable	Definición Conceptual	Definición Operacional	Dimensiones	Indicadores	Ítems
Variable A: Seguridad digital.	La ciberseguridad o seguridad digital se encarga de proteger elementos como ordenadores, servidores, documentos y cualquier otro sistema informático conectado a través de los cuales las empresas o usuarios transmiten o almacenan información valiosa (VERIDICA, 2019).	Esta VARIABLE A se va a medir mediante una ficha de investigación de elaboración propia para este estudio.	-Seguridad Digital Alta. -Seguridad Digital Media. -Seguridad Digital Baja.	Alta [26 - 45] Media [16 - 25] Baja [0 - 15]	-1; 2; 3 y 9 -4 y 5 -6; 7 y 8

Variable B: Firma Electrónica	La firma electrónica es un término que suele denotar un tipo de autenticación que sustituye a la firma física, es decir, la firma manuscrita en papel: de hecho, es la forma más sencilla de autenticar un documento, ya que utiliza medios informáticos para cumplir el consentimiento (eIDAS, 2014).	Esta VARIABLE B se va a medir mediante una ficha de investigación de elaboración propia para este estudio.	-Firma Electrónica Simple - Firma Electrónica Avanzada.	Avanzado [21 - 40] Simple [0 - 20]	-4; 5: 6; 7 y 8 -1; 2 y 3

Fuente: Elaboración propia

Anexo 05 – Resultados para la variable Seguridad Digital

Tabla 7: *Resumen de resultados variable Seguridad Digital 1 de 2*

	SEGURIDAD DIGITAL												
	D1				D2		D3						
No	P1	P2	P3	P9	P4	P5	P6	P7	P8	∑D1	∑D2	∑D3	∑TOTAL
01	5	1	1	1	1	4	1	2	3	8	5	6	19
02	4	1	1	1	1	3	1	1	3	7	4	5	16
03	4	1	1	1	1	4	1	1	3	7	5	5	17
04	5	1	1	1	1	4	1	1	2	8	5	4	17
05	5	1	1	1	1	4	1	1	3	8	5	5	18
06	5	1	1	1	1	4	1	1	2	8	5	4	17
07	4	1	1	1	1	3	1	1	3	7	4	5	16
08	4	1	1	1	1	3	1	1	2	7	4	4	15
09	4	1	1	1	1	4	1	1	2	7	5	4	16
10	4	1	1	1	1	3	1	1	3	7	4	5	16
11	4	1	1	1	1	3	1	1	2	7	4	4	15
12	5	1	1	1	1	3	1	1	2	8	4	4	16
13	4	1	1	1	1	3	1	1	3	7	4	5	16
14	4	1	1	1	1	3	1	1	2	7	4	4	15
15	5	1	1	1	1	4	1	1	3	8	5	5	18
16	5	1	1	1	1	3	1	1	2	8	4	4	16
17	4	1	1	1	1	4	1	1	2	7	5	4	16
18	4	1	1	1	1	4	1	1	3	7	5	5	17
19	4	1	1	1	1	4	1	1	2	7	5	4	16
20	4	1	1	1	1	4	1	1	2	7	5	4	16
21	4	1	1	1	1	3	1	1	3	7	4	5	16
22	4	1	1	1	1	3	1	1	3	7	4	5	16
23	5	1	1	1	1	4	1	1	2	8	5	4	17
24	4	1	1	1	1	3	1	1	2	7	4	4	15
25	5	1	1	1	1	3	1	1	3	8	4	5	17
26	4	1	1	1	1	4	1	1	2	7	5	4	16
27	5	1	1	1	1	3	1	1	2	8	4	4	16
28	5	1	1	1	1	4	1	1	2	8	5	4	17
29	5	1	1	1	1	3	1	1	3	8	4	5	17
30	5	1	1	1	1	4	1	1	3	8	5	5	18
31	5	1	1	1	1	4	1	1	2	8	5	4	17
32	4	1	1	1	1	3	1	1	3	7	4	5	16
33	5	1	1	1	1	4	1	1	3	8	5	5	18
34	4	1	1	1	1	3	1	1	2	7	4	4	15
35	5	1	1	1	1	3	1	1	2	8	4	4	16

Fuente: Elaboración propia

Tabla 8: *Resumen de resultados variable Seguridad Digital 2 de 2*

	SEGURIDAD DIGITAL												
	D1				D2		D3						
No	P1	P2	P3	P9	P4	P5	P6	P7	P8	∑D1	∑D2	∑D3	∑TOTAL
36	4	1	1	1	1	3	1	1	3	7	4	5	16
37	4	1	1	1	1	3	1	1	2	7	4	4	15
38	5	1	1	1	1	3	1	1	3	8	4	5	17
39	5	1	1	1	1	4	1	1	2	8	5	4	17
40	4	1	1	1	1	4	1	1	2	7	5	4	16
41	5	1	1	1	1	3	1	1	2	8	4	4	16
42	5	1	1	1	1	3	1	1	3	8	4	5	17
43	5	1	1	1	1	3	1	1	2	8	4	4	16
44	4	1	1	1	1	4	1	1	3	7	5	5	17
45	5	1	1	1	1	3	1	1	2	8	4	4	16
46	4	1	1	1	1	3	1	1	3	7	4	5	16
47	4	1	1	1	1	4	1	1	2	7	5	4	16
48	4	1	1	1	1	3	1	1	3	7	4	5	16
49	4	1	1	1	1	3	1	1	2	7	4	4	15
50	5	1	1	1	1	4	1	1	2	8	5	4	17
51	5	1	1	1	1	4	1	1	2	8	5	4	17
52	5	1	1	1	1	3	1	1	3	8	4	5	17
53	5	1	1	1	1	4	1	1	3	8	5	5	18
54	4	1	1	1	1	4	1	1	2	7	5	4	16
55	5	1	1	1	1	3	1	1	2	8	4	4	16
56	4	1	1	1	1	4	1	1	3	7	5	5	17
57	4	1	1	1	1	4	1	1	3	7	5	5	17
58	5	1	1	1	1	3	1	1	2	8	4	4	16
59	4	1	1	1	1	3	1	1	3	7	4	5	16
60	5	1	1	1	1	4	1	1	2	8	5	4	17
61	5	1	1	1	1	4	1	1	3	8	5	5	18
62	5	1	1	1	1	4	1	1	2	8	5	4	17
63	4	1	1	1	1	4	1	1	3	7	5	5	17
64	4	1	1	1	1	4	1	1	2	7	5	4	16
65	4	1	1	1	1	4	1	1	3	7	5	5	17
66	4	1	1	1	1	4	1	1	3	7	5	5	17
67	4	1	1	1	1	4	1	1	2	7	5	4	16
68	4	1	1	1	1	3	1	1	3	7	4	5	16
69	4	1	1	1	1	4	1	1	3	7	5	5	17
70	4	1	1	1	1	4	1	1	2	7	5	4	16

Fuente: Elaboración propia

Anexo 6 – Resultados de la variable Firma electrónica

Tabla 9: *Resumen de resultados variable Firma Electrónica 1 de 2*

	FIRMA ELECTRONICA										
	D1			D2							
No	P1	P2	P3	P4	P5	P6	P7	P8	∑D1	∑D2	∑TOTAL
01	5	2	2	1	1	1	1	1	9	5	14
02	5	1	2	1	1	1	1	1	8	5	13
03	5	1	2	1	1	1	1	1	8	5	13
04	5	1	2	1	1	1	1	1	8	5	13
05	5	1	2	1	1	1	1	1	8	5	13
06	5	2	1	1	1	1	1	1	8	5	13
07	5	1	2	1	1	1	1	1	8	5	13
08	5	1	2	1	1	1	1	1	8	5	13
09	5	2	2	1	1	1	1	1	9	5	14
10	5	2	2	1	1	1	1	1	9	5	14
11	5	2	2	1	1	1	1	1	9	5	14
12	5	2	1	1	1	1	1	1	8	5	13
13	5	2	2	1	1	1	1	1	9	5	14
14	5	1	2	1	1	1	1	1	8	5	13
15	5	1	1	1	1	1	1	1	7	5	12
16	5	1	1	1	1	1	1	1	7	5	12
17	5	2	1	1	1	1	1	1	8	5	13
18	5	2	1	1	1	1	1	1	8	5	13
19	5	2	2	1	1	1	1	1	9	5	14
20	5	2	2	1	1	1	1	1	9	5	14
21	5	1	2	1	1	1	1	1	8	5	13
22	5	2	1	1	1	1	1	1	8	5	13
23	5	1	2	1	1	1	1	1	8	5	13
24	5	1	2	1	1	1	1	1	8	5	13
25	5	1	2	1	1	1	1	1	8	5	13
26	5	2	2	1	1	1	1	1	9	5	14
27	5	1	2	1	1	1	1	1	8	5	13
28	5	2	2	1	1	1	1	1	9	5	14
29	5	2	2	1	1	1	1	1	9	5	14
30	5	1	1	1	1	1	1	1	7	5	12
31	5	2	1	1	1	1	1	1	8	5	13
32	5	1	2	1	1	1	1	1	8	5	13
33	5	1	2	1	1	1	1	1	8	5	13
34	5	1	2	1	1	1	1	1	8	5	13
35	5	1	2	1	1	1	1	1	8	5	13

Fuente: Elaboración propia.

Tabla 10: *Resumen de resultados variable Firma Electrónica 2 de 2*

	FIRMA ELECTRONICA										
	D1			D2							
No	P1	P2	P3	P4	P5	P6	P7	P8	∑D1	∑D2	∑TOTAL
36	5	2	1	1	1	1	1	1	8	5	13
37	5	2	2	1	1	1	1	1	9	5	14
38	5	1	1	1	1	1	1	1	7	5	12
39	5	1	2	1	1	1	1	1	8	5	13
40	5	1	2	1	1	1	1	1	8	5	13
41	5	1	2	1	1	1	1	1	8	5	13
42	5	2	1	1	1	1	1	1	8	5	13
43	5	1	2	1	1	1	1	1	8	5	13
44	5	2	1	1	1	1	1	1	8	5	13
45	5	2	2	1	1	1	1	1	9	5	14
46	5	2	2	1	1	1	1	1	9	5	14
47	5	1	2	1	1	1	1	1	8	5	13
48	5	2	2	1	1	1	1	1	9	5	14
49	5	1	1	1	1	1	1	1	7	5	12
50	5	1	1	1	1	1	1	1	7	5	12
51	5	1	1	1	1	1	1	1	7	5	12
52	5	2	2	1	1	1	1	1	9	5	14
53	5	2	1	1	1	1	1	1	8	5	13
54	5	1	1	1	1	1	1	1	7	5	12
55	5	2	1	1	1	1	1	1	8	5	13
56	5	1	1	1	1	1	1	1	7	5	12
57	5	1	1	1	1	1	1	1	7	5	12
58	5	2	1	1	1	1	1	1	8	5	13
59	5	1	2	1	1	1	1	1	8	5	13
60	5	1	2	1	1	1	1	1	8	5	13
61	5	2	1	1	1	1	1	1	8	5	13
62	5	2	2	1	1	1	1	1	9	5	14
63	5	1	1	1	1	1	1	1	7	5	12
64	5	1	1	1	1	1	1	1	7	5	12
65	5	1	1	1	1	1	1	1	7	5	12
66	5	1	1	1	1	1	1	1	7	5	12
67	5	1	1	1	1	1	1	1	7	5	12
68	5	2	2	1	1	1	1	1	9	5	14
69	5	2	2	1	1	1	1	1	9	5	14
70	5	1	2	1	1	1	1	1	8	5	13

Fuente: Elaboración propia.

Anexo 7 – Grado de relación según coeficiente de correlación

Tabla 11: *Grado de relación según coeficiente de correlación*

RANGO	RELACIÓN
[-0,91 a -1,00]	Correlación negativa perfecta
[-0,76 a -0,90]	Correlación negativa muy fuerte
[-0,51 a -0,75]	Correlación negativa considerable
[-0,11 a -0,50]	Correlación negativa media
[-0,01 a -0,10]	Correlación negativa débil
[0,00]	No existe correlación
[0,01 a 0,10]	Correlación positiva débil
[0,11 a 0,50]	Correlación positiva media
[0,51 a 0,75]	Correlación positiva considerable
[0,76 a 0,90]	Correlación positiva muy fuerte
[0,91 a 1,00]	Correlación positiva perfecta

Fuente: https://www.fcfm.buap.mx/SIEP/2021/Extensos%20Carteles.pdf

Anexo 8 – Muestra

Muestreo probabilístico simple:

$$\mathrm{n} = \frac{NZ^2pq}{(N-1)e^2 + Z^2pq}$$

Dónde:

n : Tamaño de la muestra $\rightarrow n = ¿?$

p : Probabilidad de éxito $\rightarrow p = 0.95$ resultado esperado según (Coronel García, 2020).

q : Probabilidad de fracaso $\rightarrow q = (1-p) \rightarrow q = 0.05$

N : Tamaño de la población $\rightarrow N = 1{,}855$

e : Error de estimación máximo aceptado $\rightarrow e = 0.05$

Z : Nivel de confianza $\rightarrow Z = 96\% \rightarrow Z = 1.96$

Tabla 12: Nivel de confianza VS $Z_\propto$

Nivel de confianza	$Z_\propto$
97.7%	3.000
99.0%	2.580
98.0%	2.330
96.0%	2.050
95.0%	1.960
90.0%	1.645
80.0%	1.280
50.0%	0.674

Fuente: http://www.vaxasoftware.com/doc/mat/dnormal.pdf

Remplazando:

$$\mathrm{n} = \frac{1{,}855(1.96)^2(0.95)(0.05)}{(1{,}855-1)0.05^2 + (1.96)^2(0.95)(0.05)}$$

$$\mathrm{n} = \frac{338.4930}{4.8175}$$

$$\mathrm{n} = 70.26$$

UNIVERSIDAD CÉSAR VALLEJO

ESCUELA DE POSGRADO

MAESTRÍA EN GESTIÓN PÚBLICA

Declaratoria de Autenticidad del Asesor

Yo, OSORIO CARRERA CESAR JAVIER, docente de la ESCUELA DE POSGRADO MAESTRÍA EN GESTIÓN PÚBLICA de la UNIVERSIDAD CÉSAR VALLEJO SAC - TRUJILLO, asesor de Tesis titulada: "La firma electrónica y la seguridad digital en los certificados de vigencia de poder emitidos por la Oficina Registral de Andahuaylas, 2022", cuyo autor es SOTELO CÁRDENAS JULIO CÉSAR, constato que la investigación tiene un índice de similitud de 20.00%, verificable en el reporte de originalidad del programa Turnitin, el cual ha sido realizado sin filtros, ni exclusiones.

He revisado dicho reporte y concluyo que cada una de las coincidencias detectadas no constituyen plagio. A mi leal saber y entender la Tesis cumple con todas las normas para el uso de citas y referencias establecidas por la Universidad César Vallejo.

En tal sentido, asumo la responsabilidad que corresponda ante cualquier falsedad, ocultamiento u omisión tanto de los documentos como de información aportada, por lo cual me someto a lo dispuesto en las normas académicas vigentes de la Universidad César Vallejo.

TRUJILLO, 30 de Diciembre del 2022

Apellidos y Nombres del Asesor:	**Firma**
OSORIO CARRERA CESAR JAVIER **DNI:** 06203497 **ORCID:** 0000-0002-2850-6420	Firmado electrónicamente por: CJOSORIOC el 12-01-2023 08:58:29

Código documento Trilce: TRI - 0505932

INVESTIGA UCV