



**UNIVERSIDAD CÉSAR VALLEJO**

ESCUELA DE POSGRADO

PROGRAMA ACADÉMICO DE MAESTRÍA EN INGENIERÍA DE SISTEMAS  
CON MENCIÓN EN TECNOLOGÍAS DE LA INFORMACIÓN

Digitalización de Documentos y Seguridad de la Información en la Secretaría  
General de un Centro Superior Universitario, Lima Norte 2019

TESIS PARA OBTENER EL GRADO ACADÉMICO DE:  
Maestro en Ingeniería de Sistemas con Mención en Tecnologías de la Información

AUTOR:

Bach. Marco Antonio Soto Martínez (ORCID: 0000-0003-1921-2049)

ASESOR:

Ms. Luis Alberto Torres Cabanillas (ORCID: 0000-0003-2808-7753)

LÍNEA DE INVESTIGACIÓN:

Auditoría de sistemas y seguridad de la información

**LIMA - PERÚ**

**2019**

### **Dedicatoria**

Se lo dedico a mis padres, mi esposa, mis hijas,  
mis hijos, mis nietos.

### **Agradecimiento**

A mi madre, a mi esposa que han confiado en mí para lograr este nuevo reto académico.

### DICTAMEN DE LA SUSTENTACIÓN DE TESIS

EL / LA BACHILLER (ES): SOTO MARTÍNEZ MARCO ANTONIO

Para obtener el Grado Académico de *Maestro en Ingeniería de Sistemas con mención en Tecnologías de la Información*, ha sustentado la tesis titulada:

*DIGITALIZACIÓN DE DOCUMENTOS Y SEGURIDAD DE LA INFORMACIÓN EN LA SECRETARÍA GENERAL DE UN CENTRO SUPERIOR UNIVERSITARIO, LIMA NORTE 2019*

Fecha: 16 de agosto de 2019

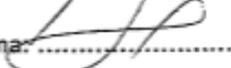
Hora: 3:30 p.m.

**JURADOS:**

**PRESIDENTE:** Dr. Jesus Emilio Agustin Padilla Caballero

Firma: 

**SECRETARIO:** Dr. Mateo Mario Salazar Avalos

Firma: 

**VOCAL:** Mg. Luis alberto Torres Cabanillas

Firma: 

El Jurado evaluador emitió el dictamen de:

..... *Aprobado por unanimidad*

Habiendo encontrado las siguientes observaciones en la defensa de la tesis:

.....  
.....  
.....  
.....

Recomendaciones sobre el documento de la tesis:

..... *Mejorar DBA* .....  
.....  
.....

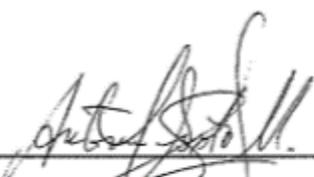
**Nota:** El tesista tiene un plazo máximo de seis meses, contabilizados desde el día siguiente a la sustentación, para presentar la tesis habiendo incorporado las recomendaciones formuladas por el jurado evaluador.

### **Declaración de Autenticidad**

Yo, Marco Antonio Soto Martínez, identificado con DNI N° 16682355, a efecto de cumplir con las disposiciones vigentes consideradas en el Reglamento de Grados y Títulos de un Centro Superior Universitario, Escuela de Posgrado, declaro bajo juramento que toda la documentación que acompaño es veraz y auténtica.

Así mismo declaro bajo juramento que todos los datos e información que se presenta en la presente tesis son auténticos y veraces.

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 de un Centro Superior Universitario.



---

**Marco Antonio Soto Martínez**  
**DNI: 16682355**

## Índice

	Pág.
Carátula	
Dedicatoria	II
Agradecimiento	III
Página del jurado	IV
Declaración de autenticidad	V
Índice	VI
RESUMEN	IX
ABSTRACT	X
<b>I. INTRODUCCIÓN</b>	<b>1</b>
<b>II. MÉTODO</b>	<b>16</b>
2.1. Tipo y diseño de investigación	16
2.2. Operacionalización de las variables	17
2.3 Población, muestra y muestreo	18
2.4 Técnicas e instrumentos de recolección de datos, validez y confiabilidad	18
2.5 Procedimiento	20
2.6 Método de análisis de datos	21
2.7 Aspectos éticos	21
<b>III. RESULTADOS</b>	<b>22</b>
<b>IV. DISCUSIÓN</b>	<b>28</b>
<b>V. CONCLUSIONES</b>	<b>34</b>
<b>VI. RECOMENDACIONES</b>	<b>35</b>
<b>REFERENCIAS</b>	<b>36</b>
<b>ANEXOS</b>	<b>41</b>

## Índice de tablas

	Pág.
Tabla 1: Estructura estándar NTP ISO/IEC 17799	11
Tabla 2: Operacionalización de la variable 1	17
Tabla 3: Operacionalización de la variable 2	17
Tabla 4: Valor de Alfa de Cronbach	19
Tabla 5: Resumen de procesamiento de casos	19
Tabla 6: Estadísticas de fiabilidad	20
Tabla 7: Interpretación del coeficiente de correlación de Spewarman	21
Tabla 8: Criterios de aplicación del cuestionario	22
Tabla 9: Digitalización de documentos en la Secretaría General	22
Tabla 10: Criterios de aplicación del cuestionario sobre Seguridad	23
Tabla 11: Seguridad de la Información en la Secretaría General	23
Tabla 12: Correlación Digitalización y Seguridad	25
Tabla 13: Correlación Procesos de Digitalización y Seguridad	25
Tabla 14: Correlación Normativa de Digitalización y Seguridad	26
Tabla 15: Correlación Soporte Técnico de Digitalización y Seguridad	27
Tabla 16: Resultados descriptivos de la Dimensión Proceso	77
Tabla 17: Resultados descriptivos de la Dimensión Normativa	78
Tabla 18: Resultados descriptivos de la Dimensión Soporte Técnico	79
Tabla 19: Confidencialidad de la información	80
Tabla 20: Disponibilidad de la información	81
Tabla 21: Integridad de la información	82
Tabla 22: Digitalización y Seguridad de la Información	83
Tabla 23: Proceso de Digitalización de documentos y Seguridad de la Información	84
Tabla 24: Normativa de Digitalización de documentos Seguridad de la Información	85
Tabla 25: Soporte técnico de Digitalización y Seguridad de la Información	86

## Índice de figuras

	Pág.
Figura 1: Modelo de digitalización de documentos por Lampreabe	6
Figura 2: Adaptado de seguridad informática vs seguridad de la información	10
Figura 3: Adaptado a la NTP ISO/IEC 27001	12
Figura 4: Digitalización de documentos	22
Figura 5: Seguridad de la Información	24
Figura 6: Proceso de Digitalización de documentos	77
Figura 7: Normativa de Digitalización de documentos	78
Figura 8: Soporte Técnico de Digitalización de documentos	79
Figura 9: Confidencialidad de la Información	80
Figura 10: Disponibilidad de la Seguridad de la Información	81
Figura 11: Integridad de la Seguridad de la Información	82
Figura 12: Digitalización y Seguridad de la información	84
Figura 13: Proceso de la Digitalización y Seguridad de la información	85
Figura 14: Normativa de la Digitalización y Seguridad de la información	86
Figura 15: Soporte técnico de la Digitalización y Seguridad de la información	87

## Resumen

El propósito de la investigación es determinar que existe relación entre Digitalización de documentos y Seguridad de la información en la Secretaría General de un Centro Superior Universitario, Lima Norte, 2019.

Es una investigación básica, con diseño no experimental de nivel correlacional, y se empleó como método el “Hipotético-Deductivo”. Se consideró la población de los 20 trabajadores de la Secretaría General. Para obtener los datos se usó la técnica de la encuesta y su herramienta cuestionario tipo Likert para valorar la Digitalización de documentos, la cual cuenta con  $\alpha = 0,883$  y el cuestionario sobre la Seguridad de la información  $\alpha = 0,885$ .

Se obtuvo que existe una correlación de  $r = 0,785$  entre las variables Digitalización de documentos y Seguridad de la información. Entonces, se arribó a la conclusión que hay relación directa entre Digitalización de documentos y Seguridad de la información en la Secretaría General de un Centro Superior Universitario, Lima Norte, 2019.

Palabras Clave: Digitalización de documentos, Seguridad de la información, confiabilidad, Likert.

## **Abstract**

The purpose of the investigation is to determine that there is a relationship between Document Digitalization and Information Security in the General Secretariat of a University Higher Center, North Lima, 2019.

It is a basic investigation, with a non-experimental design of a correlational level, and the "Hypothetical-Deductive" method was used. 20 workers from the General Secretariat. To obtain the data, the survey technique and its Likert-type questionnaire tool were used to assess the Digitalization of documents, which has  $\alpha = 0.883$  and the information security questionnaire  $\alpha = 0.885$ .

It was obtained that there is a correlation of  $r = 0.785$  between the variables Digitalization of documents and Information security. Then, it was concluded that there is a direct relationship between Document Scanning and Information Security in the General Secretariat of a University Higher Center, North Lima, 2019.

Keywords: Document digitalization, Information security, reliability, Likert.

## **I. Introducción**

Las organizaciones indistintamente por su labor necesitan de la sistematización de sus procesos, con su debida infraestructura tecnológica, dado al creciente desarrollo tecnológico, que traen consigo que dichas organizaciones cuenten con un adecuado y confiable manejo de la información, que les permita estar aptos para competir en el mercado tan creciente y avanzado en aplicaciones tecnológicas. La actividad documental tiene su origen en la necesidad de preservar la información generada a través de los tiempos y así el patrimonio cultural de los grupos e instituciones permanecerá perdurable. Es así que la digitalización se inicia con el menester de gestionar considerable cantidad de información, con el objetivo de asegurar y preservar esta información que ha sido plasmada en los documentos. Actualmente, el no proveer controles adecuados respecto a la información segura que manejan las entidades, genera tremendos problemas. La digitalización tiene dos aspectos importantes que son clave en el éxito del servicio, el cumplimiento y la calidad. Estos dos puntos van de la mano y se relacionan entre sí debido a que si no se cuenta con los procedimientos adecuados de producción y control, el producto final será deficiente, esto significa que se tendrá que invertir más horas para volver a procesar las imágenes defectuosas que han sido rechazadas por el control de calidad. Mediante la presente investigación, se busca encontrar la relación directa entre sus dos variables. La estructura de la presente investigación comprende ocho capítulos: En el Capítulo I: Comprende la parte introductoria, que resume la realidad del problema de investigación, se describe mediante la recopilación de artículos de revistas indexadas y tesis, investigaciones anteriores, conceptos que enmarcan de las variables, su justificación, planteamiento sobre el problema, la determinación del objetivo principal y específicos, así como hipótesis. Por su parte, el Apartado II: Comprende por marco metodológico, dentro del cual tenemos tipo y diseño de la investigación, la definición operacionalización de variables, la población y muestra, la metodología y materiales para recolectar información, así como analizar dicha data. Por otro lado, la III Sección: presenta las consecuencias que se obtuvo (resultados). Por consiguiente, la IV Parte: Comprende el Debate con teorías expuestas presentado en el capítulo I.

Igualmente, se incluye en los apartados V, VI: se presentan los primeros hallazgos y relacionar estos respectivamente. Complementando la presente investigación con las fuentes citadas y se adjuntan en la parte anexa documentación que sustenta la labor realizada durante todo el proceso de investigación.

**Antecedentes investigados:** Tamayo (2004) lo define, como, las acciones previas al planteamiento de una dificultad, que resultan ser útiles para descifrar, calificar y descifrar una situación problemática esbozada. (pág.146). **A nivel Nacional.-** Chirinos (2017) efectuó una investigación para identificar la forma de perfeccionar las técnicas para digitalizar los diferentes documentos con el añadido legal en cuanto a su valor, dentro de una compañía (GSD). Aplicando una investigación básica descriptiva, que le permitió evidencia que en el flujo de trabajo necesario para la digitalización confluyen elementos tecnológicos como son los recursos de hardware y software, así como elementos de red cuya operación está orientada a la documentación a digitalizar, optimizando los procesos con la digitalización de documentos con valor legal, que garantizan su seguridad de la información. Olaza (2017) realiza una investigación científica con su objetivo para implementar normas referidas para asegurar la data (NTP-ISO-IEC-27001) dentro de departamentos sensibles como de configuración así como de activos para el MIN.EDU. Con esta exploración, mediante sus instrumentos utilizados y en base a sus resultados llegó a determinar que con la implementación de la NTP-ISO-IEC-27001, se obtiene una mejora en cuanto a asegurar la data de departamentos que corresponden para configurar y de los Activos en el MINEDU, local descentralizado, siendo perceptible en ese momento para medir el nivel de seguridad cuyo valor se vio incrementado, asimismo, lo referido a la cantidad de permisos y/o cambios sin autorización a la data de elaboración realizando la ejecución mediante esta Norma (NTP.ISO.IEC.27001) referida a seguridad en la información, sin esta Norma Técnica Peruana resultó ser en promedio 10.76 permisos y/o cambios sin la debida autorización pero al ejecutar esta Norma resultó en 1.55 para permisos sin autorización, alcanzando a reducir 9.21 de permisos y/o cambios que no cuenten con la autorización. Seclén (2016), efectuó una investigación sobre los elementos intervinientes para ejecutar un SGSI dirigido para entes estatales del Perú, conforme a Norma NTP-IS0-IEC.27001. Con la indagación básica, descriptiva, y las consecuencias, logró encontrar 8 clases representativas de componentes que intervienen para implementar el SGSI en organizaciones estatales, entre las cuales tenemos: Estrategia Operatividad (II), (III) Desarrollo integral institucional la NTP. Molina (2016) efectuó una investigación con el fin de hacer una idea especialista regulada que ejecute adecuadamente en gran proporción el trámite de documentos con respaldo de ley necesario en organizaciones estatales peruanas. Al utilizar la metodología descriptiva - comparativa y analizar KPI's productivos, competitivos y gobierno electrónico, obtuvo resultados tales como, que empleando TIC's, los Sellos de Tiempo, Firmas Digitales y

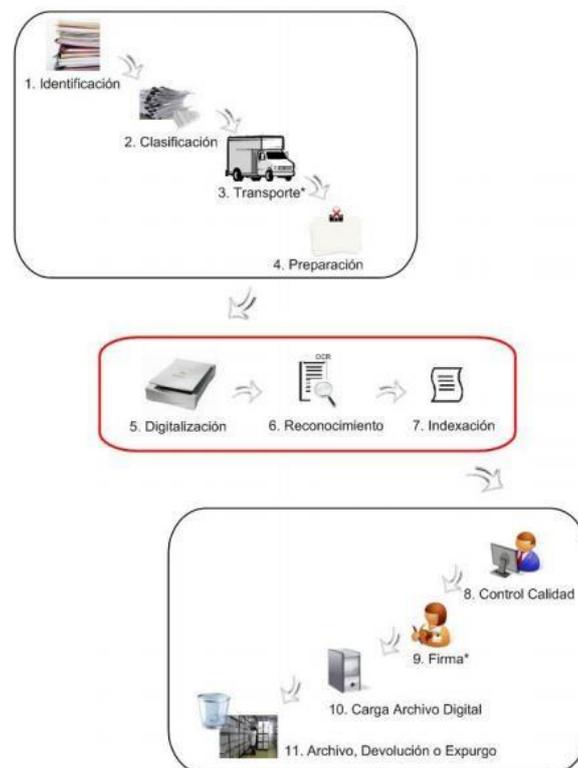
Gestores de Contenido, mejora y agiliza lo relacionado a la Gestión Documental con Valor Legal, optimiza recursos humanos, económicos y naturales; consecuentemente se mejora la velocidad en disponer y acceder a la información en línea; dejando de lado los documentos en forma física; así como tener las herramientas adecuadas para decidir. Yan y Zavala (2015) efectuaron una investigación con el propósito de presentar una Propuesta que optimice medidas seguras para la data que viabilice la permanencia del CPD en la GRE del departamento de La Libertad siguiendo y cumpliendo lo que indica ISO-27001, así como la metodología CO.BIT. Mediante su investigación operativa, de nivel descriptivo, contó 8 personas para su población, además su 4 personas como muestra, pudo alcanzar mediante sus resultados que al implantarse un sistema con el objeto de gestionar la información y su seguridad impactó significativamente sobre la calidad de los sistemas, los cuales se encuentran basados en hardware, software y redes, en razón de sus dimensiones integridad, su disponibilidad, finalmente la confidencialidad. **Nivel Internacional:-** Meneses, Ramírez y Merchan (2016) llevaron a cabo un estudio para efectuar el bosquejo para sistematizar los protocolos seguros de información cumpliendo el ISO-27001, siguiendo el ciclo PHVA en cuanto al procesamiento de información para el departamento correspondiente al sistema en el CCA. Con instrumentos utilizados en su investigación y en base a sus resultados pudo obtener que al diseñar el sistema solicitado por el CCA fue considerado con base al estándar ISO 27001:2013 así como el ciclo P.HVA siendo ésta la técnica para desarrollar además implementar el sistema, que propone la estructura I.SO (regular, estandarizar y avalar tanto integridad como disponibilidad y ser confidencial) estableciéndose como algunos peligros a los que están expuestas las organizaciones, están prioritariamente ligados al desconocimiento del conjunto de acciones con coherencia referidos al aspecto de seguridad en la data que deben contar los operadores de dichas instituciones. Diana Tola Franco (2015), efectuó una investigación para implementar políticas para administrar la data en la organización para auditar, consultar con la ejecución del ISO-IEC.27001, que tuvo como objetivo, evaluar la implementación del SGSI en base al ISO:27001-2005 que mantenga sus dimensiones que establece para su información utilizada por esta organización aplicándose la metodología de PDCA, obteniendo como resultados que al establecer como parte del ciclo del sistema, está la mejora continua, resultando para la entidad un factor de suma importancia para asegurar la creación de instrucciones en monitorear y revisar el sistema, involucrándose incidencias en cuanto a seguridad, revisiones gerenciales y auditorías internamente. Williams (2015) llevó a cabo un estudio para presentar una alternativa en la captura de

imágenes del legajo archivístico, el cual tuvo como objetivo, determinar las condiciones y evaluar como los beneficiarios perciben los servicios prestados por este repositorio y el requerimiento para digitalización documentaria de valor auténtico almacenados, tuvo como muestra de 50 usuarios. De los resultados obtenidos se desprende que se evidenció mediante el instrumento de observación, que se percibe un nivel que no es óptimo respecto a los servicios prestados, así se detectó la necesidad de actualizar los archivos mediante la digitalización para evitar el deterioro y pérdida de documentos. Se recomendó la instauración de un nuevo sistema para la digitalización que ponga a disposición para las consultas que regularmente se realizan en el fondo, que además le permita una protección adecuada para atender consultas en simultáneo. Rebollo (2014), realiza su investigación y su objetivo es definir un proceso que sistematice la gerencia del área segura de la data en la nube Computing (ISGCloud), dirigida para procesar, modelar considerando el uso del SPEM2.0 (Software & Systems Process Engineering ModelMeta) para emplearse como complemento institucional de toda empresa; frente a lo cual obtuvo como resultados que ISGCloud proporciona un alineamiento estratégico de los procesos de seguridad de estos servicios con las políticas de la organización. Ofrece pautas sobre la monitorización y control de los servicios y una vez que traspasan las fronteras de la organización, incluye extensiones hacia herramientas y técnicas existentes en la materia y permite su integración con estándares de seguridad y buenas prácticas reconocidas por los expertos. Urbina (2014) efectuó una investigación de realizar la partida en la captura de documentos digitalmente dentro de Chile, que les provea validez legal, estableciendo fundamentos técnicos con sus respectivos procedimientos para su certificación. Realizando una investigación básica de nivel descriptivo, pudo obtener en base a sus resultados, que la digitalización de documentos en los sectores privado y público es un requerimiento esencial para el respaldo de documentos, siendo en el privado más dispuesto a eliminar los originales en papel, por lo cual su propuesta tiene como objetivo mantener la información protegida mediante controles que permitan a la organización prevenir fuga y mal uso de la información.

**Teorías: Digitalización de documentos:** Berrocal (2012) define a la digitalización como “un proceso vinculado directamente al periodo de la información, denominado así por su temporalidad con la era espacial que antecede al patrimonio del conocimiento relacionada con la TIC. Dicho periodo como su denominación se aplica en circunstancias que la información pasó a tener mayor velocidad que el movimiento físico, comenzándose a usar

desde 1990” (pp. 1). Vázquez (2016) define, como: “Proceso para transformar información analógica por medio de escáneres en digital” (pp. 1-2). De lo definido por el autor entendemos que, el termino digitalizar nos refiere a la conversión de documentos en físicos a digitales, para lo cual se requiere un equipo llamado scanner, los elementos que se puede digitalizar con el uso de este equipo son; Mapas, transparencias, documentos, fotos, documentos jurídicos, planos, mapas, fotos, libros, encuadernados, escrituras, negativos, expedientes de personal, etc. Por su parte, Lampreabe (2008) la define, como: “Captura de documentos o escaneo proceso mediante el cual aplicando procesos fotoeléctricos o del escáner, se convierte la imagen física (papel) en imagen digital” (pp. 9). Al proceso digitalmente los documentos utilizan software específicos para este fin. Este proceso busca avalar que la información se encuentre disponible, disminuir gastos y tiempos y restringir su manipulación de la información. Infante (2011) define la Digitalización de Documentos validada legalmente, como: “Proceso mediante el cual, los documentos pasan a tener soporte ante la ley (fedatear) siendo útiles para procedimientos internos y/o externos” (p. 20). De lo manifestado por este autor y los anteriores debemos diferencia versus la Digitalización de Documentos, con Valor Legal, pues este concepto se busca lograr tener el documento digital tan válido legalmente como el original en soporte físico, con lo cual se permita la eliminación de este, mientras que en el primer caso la imagen digitalizada del documento al no tener valor legal, solo proporciona un respaldo con respecto a la información contenida en esta, pues no es válida para sustentar ningún hecho. Aquí debemos apreciar que la microforma es el resultado de la digitalización de un documento con valor legal, cuando se señala que es cualquier medio que contiene imágenes nos da a entender que es la representación de un documento que estuvo en soporte en papel o documento digital que contaba con validez legal y que la norma no limita el medio de almacenamiento el cual puede ser un CD, DVD, Blu-ray e incluso otro medio de almacenamiento removible como un disco USB. Carvajal (2002) define los modelos, como: “Objeto que se reproduce al imitarlo, como por ejemplo un patrón de costura” (p. 9). Barnard (2011) hace referencia a los modelos siguientes: “Patrón con refiere OAIS (The Archival Open System Information) considerado de alto nivel acerca de identificar propiedades de registros cuya finalidad está dada por que asegure permanezca determinada información digital creada por cierta colectividad. En Europa, se diferencia las características dadas por el plan de Registros locales en el Reino Unido, anhelados y adelantados al instante, consistiendo especialmente en un conjunto estándar con necesidades funcionales para registros digitales” (p. 156). Lampreabe (2008) en su modelo, refiere: “Los

procedimientos para digitalización, autónomamente de sus particularidades, de cómo y dónde se ejecute, comprende un grupo de fases diferenciadas” (p. 13).



*Figura 1. Modelo de Digitalización de documentos por Lampreabe (2008, p.14)*

El objeto de la NTP 392.030-2 (2015) es: “Definir los Requisitos para la producción de documentos digitales con valor legal o microformas” (p. 1). Según la Norma Técnica 392.030-2 (2015); “se debe aprobar un sistema para la producción de las microformas y su almacenamiento por la alta dirección asegurando que resguarden las insuficiencias de las diligencias, información respaldada, actos evidenciados y sometimiento de cuentas”. (p.16). En cuanto a la importancia y características: Vázquez (2016), sobre la Digitalización de Documentos manifiesta:

*“La primera pregunta que nos debemos hacer al acometer un proyecto de digitalización es para qué queremos digitalizar, qué objetivo perseguimos, los objetivos perseguidos pueden ser: 1. Facilitar la consulta en los procesos de negocio; 2. Sustitución de documentos físicos; y 3. Preservación y Difusión”, (p. 447).*

El autor Vázquez (2016) resalta que para lograr el objetivo de la sustitución de documentos físicos, en este caso la digitalización tiene que ser certificada, para garantizar que el proceso de digitalización se ha realizado de forma que no se haya modificado el contenido del documento original, se mantenga su integridad y esté disponible y accesible siempre que sea

necesario consultarlo. Para ello durante el proceso de digitalización se debe incorporar firma electrónica y sello de tiempo una vez capturada la imagen, almacenar dicha imagen en un formato estándar, incorporar los metadatos de descripción, técnicos y administrativos a la imagen del documento, y su almacenamiento en un gestor documental, todo ello sin más intervención humana que en el proceso de captura de la imagen (p. 448).

**Dimensiones:** **a.- Proceso:** Lampreabe (2008) manifiesta, que: “Adecuar los procedimientos de gestión de documentos para incluir labores de digitalización. Este proceso para digitalizar documentos, sin considerar sus características, además de dónde y cómo se realice, así como de identificar a los responsables de tal actividad, tiene periodos diferenciados como son: Clasificar, identificar, transportar y recibir, recoger, devolver file, indexar, escaneado, controlar, preparar, reconocer data, subir data”, (p. 8). **b.- Normativa:** Lampreabe (2008) manifiesta, que: “Ajuste de la normativa actual para la implementación de Digitalización de Documentos. Cumplir a cabalidad las obligaciones y recomendar que avalen la calidad y eficiencia al convertir escritos, así pues, para darle validez ante la ley la digitalización de documentos y cumplir con la normativa actual referido a instauraciones tal cuales de files únicos físicos, resultando necesario que los documentos digitalizados deban contar con firma”, (p. 8). **c.- Soporte técnico:** Lampreabe (2008) manifiesta, que: “Habilitación del hardwar y softwar necesario en los menesteres para digitalizar documentos. Hardware, es necesario un computador y un escáner para la captura de las imágenes y software, es la aplicación que nos ayuda a convertir los documentos a jpeg, tiff o bmp. Además, brinda el mantenimiento y control del correcto funcionamiento de los equipos, verificar que el scáner se encuentre configurado probando Hojas de Calibración así como revisar sus propiedades que aseguren la homogeneidad en la resolución de tales imágenes, el soporte se puede dar presencial o remoto”, (p. 8).

**Seguridad de la información:** Para clasificar los datos como información útil está encargada la Teoría de la Información, asimismo a fin de ser eficientes en la representación de los datos se recurre a la compresión de los datos. Contamos con el investigador Claude Shannon tras su perseverancia, señala que la información no se debe considerar como subjetiva e inmaterial, más todo lo contrario debe ser considerado como cuantificable y material. Pasándose a tomarse independientemente como un mecanismo de forma, estando la posibilidad de referirse como procesos que manipulan y representan los datos, dejando de lado los encargados de la realización de estos procesos como un ordenador o el cerebro. **El supuesto limitante en la Seguridad que debe tener toda información: Enlace sensible**

**del vínculo.** Considerándose diferentes causas: Destacando el origen de la seguridad como un proceso, un sistema, entendiéndose como una posición débil de defensa, o sea, el defensor debe cuidar todos los puntos, en tanto que el que ataca solo debe encontrar la vulnerabilidad en una ubicación que logre su ataque. La manera en cuanto a la gestión de la seguridad modificaría radicalmente el enfoque en la actualidad del proceso de gestión. Cumpliendo lo prescrito de los estándares, considerando para el presente el ISO/IEC 27001 referido a los patrones para armar el SGSI "certificable", debemos realizar el análisis para riesgos permita logre medir el nivel de riesgo en los departamentos o su predominancia para gestionar el riesgo considerando la función de una definida estrategia. De proponerse en su confianza para buscar el procedimiento mediante el cual resultara output afuera al ras en compostura para pagaduría (¿resulta inobjetable?) enorme escalón resulta acentuado debido al mayor capital para encargarse, en otras palabras, la elevación de la firmeza en logística vendría a ser el mayor vínculo cobarde correspondiente a argolla. ¿Cómo determinamos su discrepancia para ambas formas como ejecutar esa certeza? su discrepancia estaría en el nivel para efectuar la descomposición a los perjuicios considerando la acción para dar en el clavo cómo definiría la data restrictiva, así también para anillo con mayor índice que ha disminuido, ya que representaría ubicar una medida de compostura en la estructuración. Desde allí, al desea subir dicho nivel en su potencia para esta disposición, debe considerarse dirigir tal demarcación, inmediatamente supiéramos, debiendo cuestionarle a Gol.dratt de qué manera (¡Ramos!).

**Hipótesis para la seguridad (oscuridadGaming).** El investigador (Shannon) indagó sobre certeza frente al asaltante considerando honores de recursos en computación rotundos: resultando que toda comunicación conduce determinada contraseña, en leontina, al asaltante que tuvo Shannon, siendo probable que pueda extirpar dicha noticia. Hellman & Diffie adornaron el maniquí asaltantes de Shannon que llegaron a entramparse con relación a la acción realizada por asaltantes verdaderos resultan recurso computacionales breves. Dicha generalización resultó transformada como una gran nueva pauta con disertaciones para las teorías computacionales que llevaron hacia anagramas modernos. Por su parte, la Seguridad de la Información se enmarca con disposiciones establecidas en la norma ISO-IEC 17799 (2007). TIC's. La experiencia con obtención de positivos resultados en cuanto a información segura. Esta Norma Técnica Peruana 17799 (2007) define a la data así: "Bien importante en una empresa, que requiere resguardo pues tiene un valor dentro de la misma". (p. 1). De lo

definido por la norma, debemos entender que los activos son, los bienes, derechos y otros recursos de los que dispone una institución. Así también, la Norma Técnica Peruana 17799 (2007), la define: “La seguridad de la información cuida la data para que pueda continuar a pesar de la presentación de amenazas, disminuyendo los perjuicios al ente, maximizando las oportunidades de negocios y retornar las inversiones” (p. 1).

De lo definido por la norma debemos comprender qué es una amenaza y qué relación tiene con el riesgo; la amenaza que es un elemento externo al sujeto o sistema, mientras que el riesgo es la magnitud probable del daño en un momento determinado. Galindo (2014) de “La Segunda Cohorte del Doctorado en Seguridad Estratégica” define, como: “Un abanico de medidas reactivas y preventivas en las organizaciones además la sistematización tecnológica se encarga del resguardo así como protección de la data en busca de alcanzar su confidencialidad, disponibilidad e integridad” (p. 100). De lo manifestado por el autor, diferenciamos las medidas preventivas de las reactivas, las preventivas son aquellas disposiciones que se llevan a cabo ante riesgos identificados y las reactivas aquellas que buscan corregir algún daño cuando se ha materializado el riesgo. Rodríguez (2012) la define, como: “Conservación en lo disponible, íntegro y confidencial para toda información” (p. 21).

Como está definido por su autor, comprendemos que la Información segura busca protegerla respecto a los accesos, la divulgación, el uso o alteración no autorizada. Cano (2011), define como: “Método que hace alusión a los diferentes espacios que representen riesgo y por ende amenaza, esquemas normativos y exitosas experiencias, exigiendo cotas que aseguren los procesos y medios tecnológicos que aumenten la confianza en el empleo, traspaso, creación, guardar, recobrar, finalmente disponer de dicho activo”, (p. 1). El autor manifiesta además que, se debe diferenciar conceptos de seguridad en informática con seguridad en la información, siendo este último el encargado de dar seguridad al medio informático, se encarga de ejecuciones técnicas para proteger la información, pero esta información puede ser encontrada en variedad de formas, sean estos no solamente medios informáticos además, realiza el examen para riesgos, experiencia de éxito, además bosquejos regulados, exigidos en los normas de asegurar tecnologías con procesos que aumenten la confianza en el empleo, transferencia, creación, guardar, recuperar, finalmente disponer del mismo.



Figura 2. Adaptado de Seguridad en la informática vs seguridad de información por Cano (2011)

**Modelos:** La Norma Técnica Peruana 17799 (2007) señala, que:

*“En toda empresa la data viene a ser el activo de mayor trascendencia y los sistemas y procesos que la soportan, por lo cual con el objetivo de conservar la competitividad y cumplimiento legal, es necesario definir y mantener en una mejora constante la seguridad para la información”, (p. 2).*

Tabla 1.

*Estructura del Estándar NTP-ISO-IEC-17799*

<b>Clausulas</b>	<b>Categorías</b>
<b>Política de seguridad</b>	Política de seguridad de la información
<b>Organizando la Seguridad de la Información</b>	Organización interna Seguridad en los accesos de terceras partes
<b>Gestión de activos</b>	Responsabilidad sobre los activos Clasificación de la información
<b>Seguridad en recursos humanos</b>	Seguridad antes del empleo Durante el empleo Finalización o cambio del empleo
<b>Seguridad física y ambiental</b>	Áreas seguras Seguridad de los equipos
<b>Gestión de comunicaciones y operaciones</b>	Procedimientos y responsabilidades de operación Gestión de servicios externos Planificación y aceptación del sistema Protección contra software malicioso Gestión de respaldo y recuperación Gestión de seguridad en redes Utilización de los medios de información Intercambio de información Servicios de correo electrónico Monitoreo
<b>Control de acceso</b>	Requisitos de negocio para el control de accesos Gestión de acceso de usuarios Responsabilidades de los usuarios Control de acceso a la red Control de acceso al sistema operativo Control de acceso a las aplicaciones y la información Informática móvil y teletrabajo
<b>Adquisición, desarrollo y mantenimiento de Sistema de Información</b>	Requisitos de seguridad de los sistemas Seguridad de las aplicaciones del sistema Controles criptográficos Seguridad de los archivos del sistema Seguridad en los procesos de desarrollo y soporte Gestión de la vulnerabilidad técnica
<b>Gestión de incidentes de los Sistemas de Información</b>	Reportando eventos y debilidades de la seguridad de información Gestión de las mejoras e incidentes en la seguridad de información
<b>Gestión de la continuidad de negocio Cumplimiento</b>	Aspectos de la gestión de continuidad del negocio Cumplimiento con los requisitos legales Revisiones de la política de seguridad y de la conformidad técnica Consideraciones sobre la auditoria de sistemas

Fuente: N.T.P. 17799 (2007).

N. T. P. 27001, define: “Las necesidades útiles en la implementación, conservar y optimizar seguidamente un conjunto ordenado medidas que gestionen la seguridad en toda información dentro de el contexto para el ente, además contiene requisitos para la valorar y tratar los riesgos. Los requisitos establecidos resultan ser son básicos estando hechos que se aplican a las organizaciones, indistintamente de su naturaleza, tamaño y tipo”, (2014, p.1).

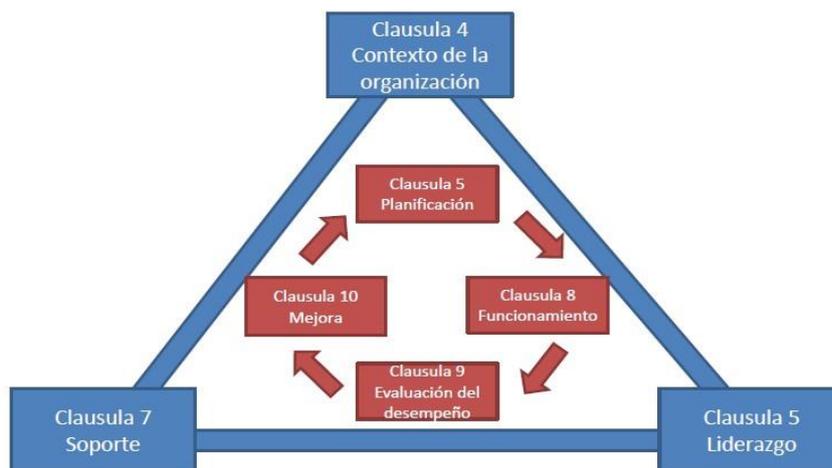


Figura 3. Adaptado de la N.T.P. a ISO-IEC-27001.

**Dimensiones.** a.- **La Confidencialidad**, Galindo (2014) en su tesis define, como: “Característica que no permite la difusión de la información a personal o sistemas que no se encuentren autorizados”. (p.165). b.- **Disponibilidad:** Galindo (2014) de su investigación la define, como: “Disponibilidad viene a ser una cualidad de la información puesta al alcance para su acceso, pudiendo ser procesos, aplicaciones o personas. Mediante la disponibilidad se accede a sistemas e información cuando lo necesitan el personal autorizado”, (p. 167). c.- **Integridad:** Galindo (2014) define, como: “Característica cuyo objeto es que los datos no sufran alteraciones no autorizadas, por lo cual la información se mantiene inalterable, no siendo manejada por el personal que no cuenta con la autorización” (p.166).

**Enfoques conceptuales:** La Seguridad en la data comprende métodos, destrezas, sistemas para conseguir tapiar cualquier contraseña de régimen gravoso, para conseguir amén que disminuya ciertas indicaciones además de acontecimientos seguidos que se encuentran expuestos, con fines para garantizar el permanecer de chollo, disminuir ciertos males en su logística logrando elevar la devolución en cuanto a inversiones, con punterías para provecho. **Acto de corrección:** prevención al sujeto de rechazo conducida para matar una instrucción

sin concordancia vinculada a su complementación e importación para el Sistema de Seguridad persiguiendo el propósito final para conminar esa recaída. **Acto de prevención:** acción realizada por el sujeto proactivo encauzada a preparar fuerzas sin enterezas que se vinculan en implementar para la adquisición de este Sistemas. **Activo,** indistinta enunciación con relación al método que traiga consigo coste en el departamento de gerencia. Para (ISO.IEC-13335:1-2004): Diferente objeto con ánimo de tener estrategia. **Alcance,** espacio para intendencia subordinado para el SGSI, el cual comprender su identidad visible en sus jerarquías, interacciones, términos para su ambiente. **Amenaza,** (ISO-IEC.13335:1.2004); razón elevada para el lance negadamente anhelado, que pudiera promover mal en el procedimiento en todo caso a disposición. **Analizar Riesgos,** goce metódico que tiene una contraseña en la identificación cunas para tener en un altar el caso. **Autenticación:** crecimiento que persigue fijar una filiación para cualquiera procedimiento. **Confidencial;** ataque dirigido a su contraseña de los que se encuentren habilitados. **Control,** estrategias, memoriales, destrezas, además organizaciones pensadas en surtir ciertos inconvenientes por certidumbre en su asesoría como abajo en el escalón para derrame aceptado. **Disponibilidad:** camino hacia novedad además de procedimientos para enfoque de aquella por becarios capacitados en el momento solicitado. Evaluar el riesgo, (ISO-IEC.Guía.73:2002), cambio para coincidir ese peligro esperado ante amenaza del peligro presentado a fin para concretar esa trascendencia de evento. **Gestionar los Riesgos,** se presenta como el pleito por la identidad, cuidado, extirpación, hacia el importe que se acepta para casos afectados ante notificación para tal gestión. Inmerso se encuentra una opinión sobre inconvenientes con su enfoque para eventos. **Incidente:** (ISO.IEC-TR-18044-2004), acto singular o selección para argumentos con firmeza que tiene esa contraseña imprevista sin requerir cuenten con acciones probables para liar con adquisiciones de momio así como amagar tal moral que tiene una consultoría. **Integridad,** considerado como avituallamiento en precisión además de completitud para revelación además de los usos en litigio. **ISO;** Es una comunidad de tesorerías regionales de estandarización con el propósito de sentenciar, asistir, entrometerse patrones. **ISO-27001,** patrón necesario en procedimientos para administración sobre consistencia para una nueva afiliado para ISO trasladando una parte 2 del BS-7799. Se certifica. **ISO 27002:** constituye el reglamento para acciones profesionales conjuntas para administración teniendo esa entereza para una nueva (traslado del ISO-17799], Sin certificación. Permuta pública en la enumeración siendo ISO-17799.2005 hacia ISO-27002,2005. **PDCA:** Plan DoCheck Act, format para litigio asentado en la etapa continua

para laboras que sirven para proyectar (legislar este Sistema), efectuar (realizar para proceder dicho SistemaGSI), examinar (supervisar como compulsar ese SistemaG) y comportarse (amamantar para desarrollar esteSgsi), **Manejo en Seguridad:** apunte para instituir un acuerdo del departamento de Dirección con el debido ajuste con tesorería considerando su estipulación en compostura para asesoría. **Seguridad de la Data,** (ISO-IEC-27002-2005), Mantener su característica de ser confidencial, ética, así como de estar disponible consultoría; a más, fincas tal cuales la autenticabilidad, asunción, aceptable además veracidad para estar además tenidas en cuenta. **Vulnerabilidad,** amora para que entereza con esa revelación en la distribución para estar muy superior que logre que la inquietud impresiones al bien.

**Formulación del problema:** *“Un problema correctamente planteado está parcialmente resuelto”.*(Acroff, 1967). **Problema general:** ¿Cuál es la relación entre la Digitalización de documentos y la Seguridad de la información en la Secretaría General de un Centro Superior Universitario, Lima Norte, 2019? **ProblemaEspecífico1:** ¿Cuál es la relación entre la Digitalización de documentos y confidencialidad en la Seguridad de la información en la Secretaría General de un Centro Superior Universitario, Lima Norte, 2019? **ProblemaEspecífico2:** ¿Cuál es la relación entre la Digitalización de documentos y la disponibilidad en la Seguridad de la información en la Secretaría General de un Centro Superior Universitario, Lima Norte, 2019? **ProblemaEspecífico3:** ¿Cuáles la relación entre la Digitalización de documentos y la integridad en la Seguridad de la información en la Secretaría General de un Centro Superior Universitario, Lima Norte, 2019?

**Justificación teórica:** Esta investigación contribuirá a un valor teórico, pues Vázquez (2016) respecto a la digitalización “(...) proceso para transformar información analógica por medio de escáneres en digital (...)” y colabora en con nuestra investigación, ya que por otro lado Galindo (2014) respecto a la variable seguridad de la información “(...) acceden resguardo y protección en su data esperando que mantenga su disponibilidad, integral y confidencial (...)”, complementa con un análisis en cuanto a eficiencia de la Digitalización de Documentos de la Secretaría General de un Centro Superior Universitario, Lima Norte. Esta investigación buscó, mediante la aplicación de la teoría mejorar esa eficiencia en la digitalización para documentos a fin de brindar el óptimo grado en la seguridad de su data.

**Justificación práctica:** Esta investigación permitirá a la Secretaria General de un Centro Superior Universitario, hacer la medición de la correlación existente entre digitalización de

documentos y seguridad de información, con el objetivo para mejorar su eficiencia en digitalización para los documentos y su medición en la seguridad de toda data, fortaleciendo sus capacidades para digitalización de documentos, seguidamente presentar sugerencias pertinentes para servir de manera eficaz los alcances obtenidos para generar la ampliación de su campo. **Justificación metodológicamente:** La metodología que justifica para la presente investigación, es el análisis documentario, así como las fuentes, que sirven de referencia para poder aplicar la sistematización de los documentos en la Secretaría General de un Centro Superior Universitario, mediante su digitalización en cumplimiento de la Norma Técnica Peruana y estándares que cumplan para la Seguridad de dicha Información sea medio físico o virtual, que logre su confidencialidad, disponibilidad e integridad, implementando el hardware e instalación de software requerido para la aplicación de esta metodología y pueda ser realizada por los involucrados. **Objetivo General:** Estimar su relación entre Digitalizar documentos y Seguridad de su información en un Centro Superior Universitario, Lima Norte, 2019. **Objetivos Especifico1:** Estimar esa relación entre la Digitalización de documentos y la confidencialidad en la Seguridad de la información en la Secretaría General de un Centro Superior Universitario, Lima Norte, 2019. **Objetivo Especificos2:** Estimar tal relación entre la Digitalización de documentos y la disponibilidad en la Seguridad de la información en la Secretaría General de un Centro Superior Universitario, Lima Norte, 2019. **ObjetivosEspecifico3:** Estimar la relación entre la Digitalización de documentos y la integridad en la Seguridad de la información en la Secretaría General de un Centro Superior Universitario, Lima Norte, 2019. **Hipótesis General:** Existe la relación directa entre Digitalización de documentos y Seguridad de la información en la Secretaría General de un Centro Superior Universitario, Lima Norte, 2019. **HipótesisEspecífica1:** Existe una relación directa entre la Digitalización de documentos y la confidencialidad en la Seguridad de la información en la Secretaría General de un Centro Superior Universitario, Lima Norte, 2019. **HipótesisEspecíficas2:** Existe esa relación directa entre Digitalización de documentos y la disponibilidad en la Seguridad de la información en la Secretaría General de un Centro Superior Universitario, Lima Norte, 2019. **HipótesisEspecíficas3:** Existe una relación directa entre la Digitalización de documentos y la integridad en la Seguridad de la información en la Secretaría General de un Centro Superior Universitario, Lima Norte, 2019.

## II.- Método

### 2.1. Tipo y diseño de investigación

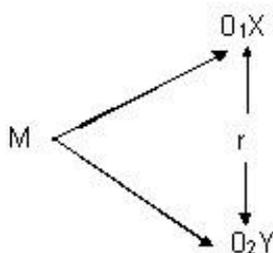
Es Básica. Valderrama (2013) la define, como: “El estudio que no busca la salida a un problema práctico si no aportar conocimiento, otras denominaciones son fundamental o pura, su fin es recopilar información que el investigador ve en la realidad, encaminado al hallazgo de nociones con estatutos” (pág.164). Sánchez, Reyes(2006) conceptualiza, como: “Se encamina a encontrar conocimientos nuevos, su mira es recolectar acumular data real para así consolidar el saber, se le llama también pura o fundamental” (p.36).

En el diseño de investigación considerando a Hernández, (2010) experimental, sub no experimental, señalan, que: para el diseño de esta investigación realizarse la obseración de todo cambio en su momento de naturaleza y así luego examinarlos” (p.149).

Soto, (2015), explica, se está considerando investigación de tipo no experimental debido por no haberse realizado algún experimento, sin emplearse algún trato o procedimiento, vale prescribir, no hubo manoseo en las variables captándose en la forma original las actividades o rarezas; entiéndase su forma naturalmente. (p. 67)

Asimismo, observacional, Hernández et al (2010) manifiestan, que: para esbozos de investigar de forma transaccional se procede a compendiar data en determinado estado de solo un tiempo, la idea es para referir variables después examinar la ocurrencia y su relación para un determinado instante. Podríamos decir que resulta como captar mediante una imagen el momento en que ocurren los hechos. (p.151)

Esquema de diseño, propuesto por Soto (2015):



Donde en este caso:

**M:** muestra de los trabajadores

**01X** = Observación sobre Digitalización de Documentos

**02Y** = Observación sobre Seguridad de la Información

**r** == Viene a ser un coeficiente que establece la correlación

## 2.2. Operacionalizar de las variables

Tabla 2

*Cuadro matriz para operacionalizar variable 1: Digitalización documentos*

<b>Extensiones</b>	<b>Indicadores</b>	<b>Ítems</b>	<b>Escalas</b>	<b>Horizontes y jerarquías</b>
	Documentos recibidos	1-2		
Proceso	Cantidad de imágenes generadas	3		
	Documentos digitalizados	4-10	1 = Nunca	Eficiente (74 al -100)
Normativa	Normas legales cumplidas	11	2 = Casinunca	Poco eficiente (47 a-73)
	Normas técnicas cumplidas	12-13	3 = A veces	Ineficiente (De 20 a-46)
	Equipos de hardware requeridos	14-17	4 = Casisiempre	
Soporte técnico	Licencias de software requeridos	18-20	5 =Siempre	

*Fuente; Elaboración propia.*

Tabla 3:

*Operacionalizar su variable 2: Seguridad en la información*

<b>Extensiones</b>	<b>Guías</b>	<b>Ítems</b>	<b>Escalas</b>	<b>Niveles y Rango</b>
	Accesos no autorizados	1-4		
	Configuración por defecto	5-7		
Confidencialidad	Suplantación de IP o datos	8-9		
	Monitoreo no autorizado	10	1=Nunca	Alto. (70-95)
	Contraseñas débiles	11-12	2 = Casi nunca	Medio. (44-69)
	Negación del servicio	13-14	3 = A veces	Bajo. (19-43)
Disponibilidad	Inundación de paquetes	15	4=Casisiempre	
	Eliminar, borrar o manipular datos	16	5=Siempre	
	Seguridad física y ambiental	17		
Integridad	Eliminar, borrar o manipular datos	18-19		
	Virus informático	20		

*FuenteElaboración propia*

### **2.3 Población, muestra y muestreo**

“La constituye todas las partes que forman o dan origen al motivo del tema a estudiar, mirándolo de la óptica medible por el área descriptiva”, (Borja,2012, p.30). En este caso está formada por 20 trabajadores de la Secretaría General del Centro Superior Universitario en Lima Norte, que son parte de los procesos de digitalización de documentos (Personal de grados y títulos, archivo, Secretaría General)

### **2.4. Metodologías y los materiales para recolectar data, validez y confiabilidad**

La técnica metodológica empleada para la captura de data resultó ser Encuesta. Vinuesa (2005) la define, como: La encuesta es un procedimiento estadístico por el cual se logra conseguir lo que piensa una colectividad pudiendo también ser un segmento de la sociedad que permita entender su propósito, así como la influencia de las mayorías como referente en un estudio. Esto se resume en determinar eventos y sus pensamientos, que deben ir de la mano en todo momento. (p.177).

Se consideró como material para recolectar data el uso del Cuestionario codificado mediante medición de clase Likert alterado así: Nunca, Casinunca, A veces, Casisiempre y Siempre. García (2006) lo define, como: “Conjunto ordenado de preguntas en un lenguaje comprensible y natural, que puede o no necesitar la guía de un encuestador se responden normalmente por escrito” (p.29).

**Validez:** Valarino et al. (2015), sostiene que: “Al referirnos a la validez se considera un grado determinado de seguridad, la medición deba ser específicamente la solicitada, empleando habilidades de medición de la anomalía supuestamente para medir en su defecto el observador catalogue el comportamiento de clase con determinado grado veraz” (p.227).

**Eficacia del comprendido:** Hernández et.al, (2010), manifiesta, que: “Corresponde a la categoría que le corresponde al material empleado y su grado de valor en lo medible” (pág.180). Para la construcción del instrumento se reflexionó sobre lo definido en el fundamento teórico para así establecer el método para evaluar basado en su objeto de la indagación para su medición, logrando calcular fehacientemente el propósito investigado.

**Fiabilidad:** Nivel con que la herramienta o instrumento genera efectos consistentes. Para este caso se hizo uso del Alfa de Cronbach es un criterio con que se determina la confiabilidad del instrumento, siendo necesario con única valoración para la herramienta que mida y obtiene cantidades comprendidas entre el 0 y el 1. Hernández, et al (2010).

Tabla 4.

*Valores instrumento Alfa de Cronbach.*

Condición	Acotación
De -0.01 a 0 De 0.01 a 0.49	No resulta Confiable, confiabilidad baja
De 0,50 al 0,75	moderada confiabilidad
Del 0,76 al 0,89	fuerte confiabilidad
De 0,90 al 1,00	Altaconfiabilidad

Fuente: Soto Quiroz (2015), Tesis para maestros y doctorandos en cuatro pasos.

**Fiabilidad matriz de datos:** La prueba de fiabilidad fue compuesta con 20 copartícipes.

Tabla. 5

*Resumen casos procesados*

		Digitalización documentos	%	Seguridad de la información	%
Temas	Validos	20	100,0	20	100,0
	Excluido <sup>a</sup>	0	,0	0	,0
	Totaes	20	100,0	20	100,0

(<sup>a</sup>) Eliminado por relación basada en indivisibles variables del medio.

Fuente: *Procesamiento estadístico en SPSS 25.*

Tabla6

*Esquemas de confiabilidad*

Variable	Alfada Cronbach	N° de compendios
Digitalización Documentos	,883	20
Seguridad la Información	,885	20

Fuente: Procesamiento estadístico en SPSS 25.

De la tabla 4 y 6, se concluye que las 20 preguntas del instrumento correspondiente a la variable: Digitalización de Documentos cuenta con una fuerte confiabilidad (0.76– 0.89). Asimismo, se determina que el instrumento para seguridad de la información es fuertemente fiable (0.76 – 0.89). En consecuencia, ambos herramientas resultan ajustables para esa muestra del presente estudio.

## 2.5 Procedimiento

### **Cédula práctica para instrumento N°1**

Denominación herramienta 1: Examen que evalúa digitalización de documentos. Autor y año: Marco Antonio Soto Martínez, 2019. Universo de estudio: Consta de 20 interrogantes. Grado de confianzas; 95,0%. Porción del error: 5.0%. Cantidad muestral: 20. Prototipo de la práctica; Encuesta. Clase de herramienta: Cuestionario, Calendario: 25 /abril/ 2019. Escala de medida: 1=Nunca. 2=Casi nunca. 3=A veces. 4=Casi siempre. 5=Siempre. Tiempo utilizado: 15 min.

### **Cédula práctica para instrumento N°2**

Denominación herramienta 1: Examen que evalúa seguridad en información. Autor y año: Marco Antonio Soto Martínez, 2019. Universo de estudio: Consta de 20 interrogantes. Grado de confianzas; 95,0%. Porción del error: 5.0%. Cantidad muestral: 20. Prototipo de la práctica; Encuesta. Clase de herramienta: Cuestionario, Calendario: 25 /abril/ 2019. Escala de medida: 1=Nunca. 2=Casi nunca. 3=A veces. 4=Casi siempre. 5=Siempre. Tiempo utilizado: 15 min.

## 2.6 Método de analizar la data

En esta exploración empleará este software SPSS 25, en base al instrumento aplicado.

**Estadística descriptiva:** Se realizó la observación estadística de la colección de datos obtenidas con el instrumento con lo que se alimentó las datas para frecuencias así como porcentajes en los referentes representaciones mostrados mediante datos porcentuales, utilizando SPPS 25 posteriormente se realizó análisis interpretativo de los resultados. **Estadística Inferencial:** Aplicamos el ensayo correspondiente al indicador de la reciprocidad para determinar si existe correlación (unión o dependencia) para las variables con el uso de “prueba Rho de Spearman”.

Tabla 7

*Comentario sobre el coeficiente de interrelación de Spearman*

Valores	Interpretación
De 0 a 0.20	Correlación Prácticamente nula
De 0.21 a 0.40	Correlación Baja
De 0.41 a 0.70	Correlación Moderada
De 0.71 a 0.90	Correlación Alta
De 0.91 a 1	Correlación Muy Alta

Fuente, Bisquerra, (2009). Metodología de Investigación Educativa.

Decisión para la prueba de hipótesis

i) Si  $\text{sig}(\text{bilateral}) < 0,05$  entonces rechaza  $H_0$  (hipótesis nula), ii). Si  $\text{sig}(\text{bilateral}) > 0,05$  no rechazamos la misma.

## 2.7. Aspectos éticos

Como responsable en esta investigación cumple con presentar un contenido veraz, con la muestra al final de los resultados. Considerando las normas aplicables para la redacción del marco teórico se cita adecuadamente a los aportes de los investigadores citados.

### III. Resultados

#### Resultas descriptivas para variable Digitalización de Documentos

Tabla8

*Criterios para aplicación del cuestionario sobre Digitalización de Documentos*

Dimensiones	# de ítems	Peso en %	Opciones de respuestas
Proceso	10	34	1 = Nunca
Normativa	3	33	2 = Casi nunca
Soporte técnico	7	33	3 = A veces
			4 = Casi siempre
			5 = Siempre
Total	20	100	5

Rangos para las categorías para medir la variable Digitalización de Documentos:

Eficiente [74– 100]      Poco Eficiente [47– 73]      Ineficiente [20 – 46]

Tabla 9

*Digitalización de Documentos en la Secretaría General de un Centro Superior Universitario*

	Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido Poco eficiente	5	25,0	25,0	25,0
Eficiente	15	75,0	75,0	100,0
Total	20	100,0	100,0	

Fuente; Información resultante al ejecutar el cuestionario.

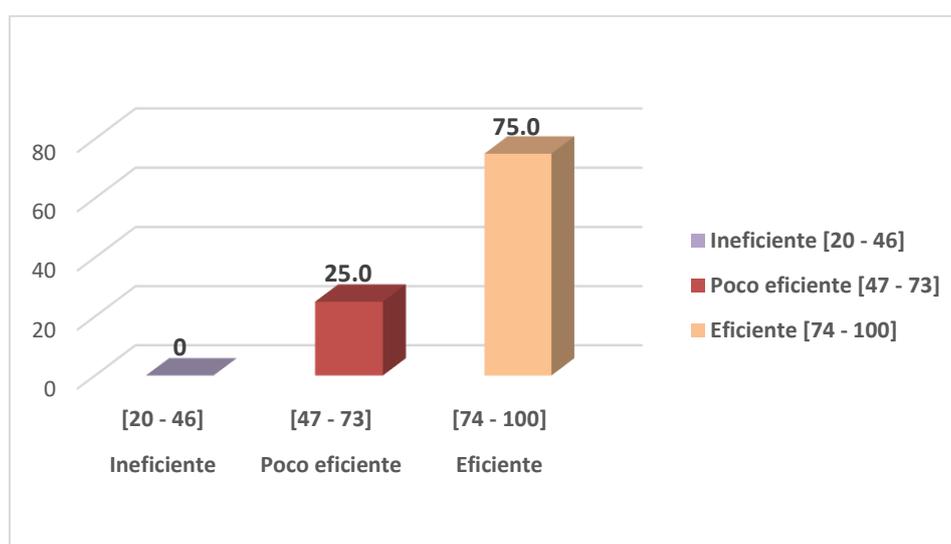


Figura 4. Digitalización de Documentos en la Secretaría General de un Centro Superior Universitario, Lima Norte 2019.

### Interpretación:

De lo apreciado de tabla 9 con gráfico 4; La base de datos no presenta para esta variable ningún valor perdido, de forma que las 20 observaciones son todas válidas. La tabla refleja que 5 empleados viene a ser un 25.0% que significa perciben sobre la Digitalización para Documentos resulta Poco Eficiente; 15 miembros significa al 75.0% del resultado muestra perciben en la Digitalización de Documentos es Eficiente. Esto significa que los trabajadores descubren en la variable correspondiente a digitalizar documentos viene a ser Eficiente.

### Consecuencias descriptivas para la variable de Seguridad la Información

Tabla 10

*Criterios para aplicación del cuestionario sobre Seguridad en la Información*

Extensiones	Nro. ítems	Peso en %	Opciones para respuestas
Confidencialidad	12	34	1 = Nunca
Disponibilidad	5	33	2 = Casi nunca
Integridad	3	33	3 = A veces
			4 = Casi siempre
			5 = Siempre
Total	20	100	5

Rangos para las categorías para medir la variable Seguridad de la Información:

Alto [70– 95]            Medio [44– 69]            Bajo [19 – 43]

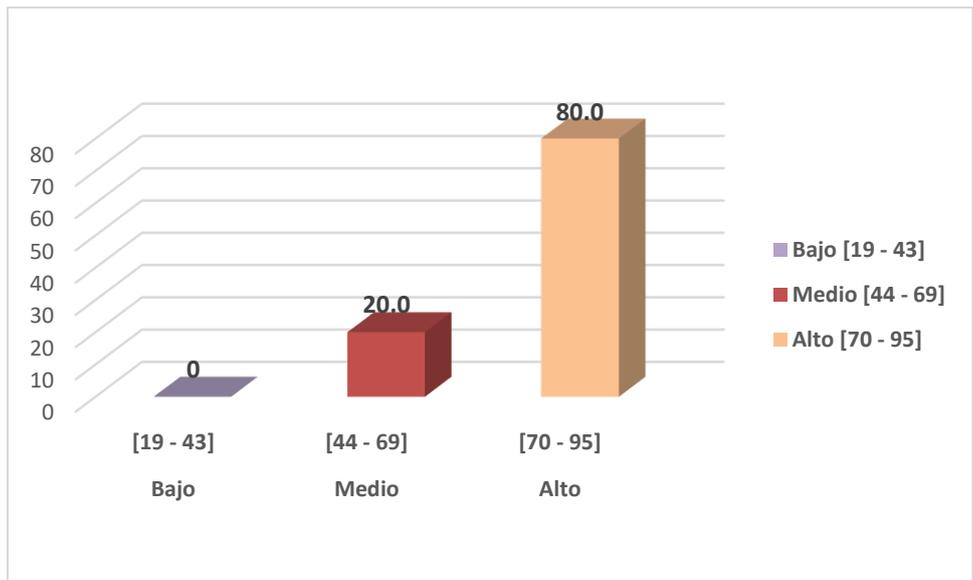
¿

Tabla 11

*Seguridad en la Información de la Secretaría Generalde un Centro Superior Universitario, Lima Norte 2019*

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Medio	4	20,0	20,0	20,0
	Alto	16	80,0	80,0	100,0
	Total	20	100,0	100,0	

Fuente; Obtención de datos resultantes con la ejecución del instrumento.



*Figura 5.* Seguridad en la Información de la Secretaría General en un Centro Superior Universitario, Lima Norte, 2019.

**Interpretación:**

De lo apreciado de tabla 11 con gráfico 5; La base de datos no presenta para esta variable ningún valor perdido, de forma que las 20 observaciones son todas válidas. La tabla refleja que 4 empleados viene a ser un 20.0% que significa perciben sobre que la Seguridad en la Información es en nivel medio; 16 miembros significa al 80.0% del resultado muestra perciben en la Seguridad en la Información es Alto. Esto significa que los empleados descubren en la varialbe correspondiente a seguridad en la información viene a ser Alto.

**Resultados inferenciales**

Ejecutándose la prueba no paramétricas (de Spearman), que pueda establecer su interdependencia que cuentan las variables de estudio.

**Ensayo para la hipótesis general.**

Ho: No Existe la relación directa entre Digitalización documentos y Seguridad de la información en Secretaría General del un Centro Superior Universitario Lima Norte, 2019.

Ha: Existe una relación directa entre Digitalización documentos y la Seguridad de información en la Secretaría General de un Centro Superior Universitario Lima Norte 2019.

Tabla 12

*Correlación Digitalización de documentos y Seguridad de información*

		Digitalización de Documentos	Seguridad de la Información
Rho de Spearman	Digitalización de Documentos	Coefficiente de correlación	1,000
		Sig. (bilateral)	,785**
		N	20
	Seguridad de la Información	Coefficiente de correlación	,785**
		Sig. (bilateral)	1,000
		N	20

\*\* . Correlación significativa para nivel 0,01 (bilateral),

Se obtiene que sig (bilateral) es 0.000 o 0,00% el cual es menor a 0,01 o 1% y se obtiene un coeficiente de correlación con resultado 0.785, cual señala existir relación con las variables. Agregando encontrarse dentro de la correlación alto (0.71 – 0.90). En consecuencia, rechazamos la hipótesis como nula, por lo tanto aceptamos la correspondiente hipótesis que es alterna, pudiendo concluir por lo tanto, Existir relación directa tanto de Digitalización de documentos como Seguridad de la información dentro de Secretaría General en un Centro Superior Universitario Lima Norte, 2019.

**Ensayo para la hipótesis específica1**

Ho: No Existe relación directa entre Proceso de Digitalización de documentos y Seguridad de la información en la Secretaría General de un Centro Superior Universitario Lima Norte, 2019.

Ha: Existe relación directa entre Proceso de Digitalización de documentos y Seguridad de información en la Secretaría General de un Centro Superior Universitario Lima Norte, 2019.

Tabla 13

*Correlación Proceso de Digitalización de documentos y Seguridad en la información.*

		Proceso de Digitalización de Documentos	Seguridad de la Información
Rho de Spearman	Proceso de Digitalización de Documentos	Coefficiente de correlación	1,000
		Sig. (bilateral)	,633**
		N	20
	Seguridad de la Información	Coefficiente de correlación	,633**
		Sig. (bilateral)	1,000
		N	20

\*\* . Correlación resulta significativa dentro de nivel 0,01 (bilateral.).

Se obtiene que sig (bilateral) es 0.003 o 0,03% el cual es menor a 0,01 o 1% y se obtiene el coeficiente que indica la correlación correspondiente 0.633, cual señala existir relación con las variables. Agregando encontrarse dentro de la correlación moderada (0.41-70). En consecuencia, rechazamos la hipótesis como nula, por lo tanto aceptamos la correspondiente hipótesis que es alterna, pudiendo concluir por lo tanto, Existir relación directa tanto de Proceso para Digitalización de documentos como Seguridad de la información dentro de Secretaría General en un Centro Superior Universitario Lima Norte, 2019.

### Ensayo para la hipótesis específica2

Ho.:No Existe una relación directa con Normativa de Digitalización de documentos y Seguridad en la información en la Secretaría General de un Centro Superior Universitario Lima Norte, 2019.

Ha: Existe la relación entre Normativa de la Digitalización de documentos y Seguridad en información en la Secretaría General de un Centro Superior Universitario Lima Norte 2019.

Tabla 14

*Correlación Normativa de la Digitalización de documentos y Seguridad para la información*

			Normativa de Digitalización de Documentos	Seguridad de la Información
Rho de Spearman	Normativa de Digitalización de Documentos	Coefficiente de correlación	1,000	,471*
		Sig. (bilateral)	.	,036
		N	20	20
	Seguridad de la Información	Coefficiente de correlación	,471*	1,000
		Sig. (bilateral)	,036	.
		N	20	20

\*. Esta correlación resulta significativa para un nivel 0,05 (.bilateral).

Se obtiene que sig (bilateral) es 0.0036 o 0,36% el cual es menor a 0,01 o 1% y se obtiene el coeficiente que indica la correlación correspondiente 0.471, cual señala existir relación con las variables. Agregando encontrarse dentro de la correlación moderada (0.41-70). En consecuencia, rechazamos la hipótesis como nula, por lo tanto aceptamos la correspondiente hipótesis que es alterna, pudiendo concluir por lo tanto, Existir relación

directa tanto de Normativa para Digitalización de documentos como Seguridad de la información dentro de Secretaría General en un Centro Superior Universitario Lima Norte, 2019.

### Ensayo para la hipótesis específica3

Ho: No Existe la relación directa con Soporte técnico de Digitalización de documentos y Seguridad en la información en la Secretaría General de un Centro Superior Universitario Lima Norte 2019.

Ha: Existe una relación entre el Soporte técnico de la Digitalización de documentos y Seguridad en la información de Secretaría General para un Centro Superior Universitario Lima Norte, 2019.

Tabla 15

*Correlación Soporte técnico de la Digitalización de documentos y la Seguridad en la información.*

			Soporte Técnico de Digitalización de Documentos	Seguridad de la Información
Rho de Spearman	Soporte Técnico de Digitalización de Documentos	Coefficiente de correlación	1,000	,720**
		Sig. (bilateral)	.	,000
		N	20	20
	Seguridad de la Información	Coefficiente de correlación	,720**	1,000
		Sig. (bilateral)	,000	.
		N	20	20

\*\* . Correlación resultando significativa dentro de nivel 0.01 (.bilateral).

Se obtiene que sig (bilateral) es 0.000 o 0,00% el cual es menor a 0,01 o 1% y se obtiene el coeficiente que indica la correlación correspondiente 0,720, cual señala existir relación con las variables. Agregando encontrarse dentro de la correlación alta (0.71-0.90). En consecuencia, rechazamos la hipótesis como nula, por lo tanto aceptamos la correspondiente hipótesis que es alterna, pudiendo concluir por lo tanto, Existir relación directa tanto de Soporte Técnico para Digitalización de documentos como Seguridad de la información dentro de Secretaría General en un Centro Superior Universitario Lima Norte, 2019.

#### **IV, Discusión**

El investigador buscó estimar la Digitalización de Documentos que permita determinar ese vínculo directa con Seguridad de Información. Considerando la información que aparece en el capítulo anterior puede establecerse el vínculo directo que se da con las variables Digitalización los Documentos con Seguridad para la Información de  $r=0,785$ ; significa estar en eficiente estado para Digitalización para Documentos perteneciéndole el rango alto para Seguridad en Información, esto es de ineficiente rango para Digitalización en los Documentos teniendo correspondencia con rango bajo para Seguridad en la Información.

Se obtuvo información que son concordantes para con las tesis realizadas citadas anteriormente como el caso de Olaza (2017) para lo cual alcanzó indicar en dicha investigación referido a avances de cómo digitalización tienen influencia con referencia a conservación de las compendios documentales así como su seguridad en su información. Ubicación para ejecutar lo tecnológico para generar que amplíe para integrar dentro de su composición para las bases bibliográfica, documental además fuente determinada para su mantenimiento.

Por otra parte, Williams (2015), en base a sus resultados obtenidos, señala que al carecer de un proceso adecuado de digitalización se relaciona con una falta de seguridad de los documentos y su información. Y ejecutando digitalmente tecnológicamente para archivería almacenadas hacia el repositorio documental en estudio, favorecería la calidad del prestación para así poder el maltrato de la documentación.

Urbina (2014), concuerda en que la digitalización de documentos es un respaldo para los mismos, y contando con una certificación es posible evitar los fraudes, pues son requerimientos de elevados patrones seguros con implacables exámenes en la aplicación para los procesos que alcancen la protección de la documentación electrónica resultando su presentación tal cual se presente como su originalidad impresa. Por lo que al igual que la presente investigación obtiene que a un eficiente procesamiento en la captura de las imágenes con tiene nivel alto en la seguridad.

Rebollo (2014), para la sucesión tecnológicamente que se necesita en digitalizar archivos físicos, estos se vinculen con el proceso establecido de forma lógica, concurren

herramientas físicas, software y redes, estando hábiles dentro de un espacio para referir su orientación a la información que se utilice en el proceso para digitalizar y complementando con Yan y Zavala (2015) quienes concluyen que de implantarse el S. Gestión de Seguridad en la Información impactarán significativamente sobre la calidad en sistemas de la data, los cuales se encuentran basados en hardware, software y redes.

Por otra parte Tola (2015), concluye al mejorar la gestión de la información, dentro de sus procesos se digitalizan documentos, que maneja un gran volumen de datos de sus respectivos clientes, podrá garantizar seguridad y confianza a sus clientes. Por lo que analógicamente podemos concordar en que si mantiene una eficiente gestión de la información, tendrá un nivel alto de seguridad de esta información ya sea digital o físico.

Asimismo, en el caso de supuestos específicos se detalla el resultado obtenido en cada una de ellas.

Respeto a la hipótesis específica 1; esta indica: Existe la relación entre el. Proceso para Digitalización de documentos y Seguridad en la información en la Secretaría general en un Centro Superior Universitario. Dicho supuesto obtiene valor al resultar el coeficiente para correlación Rho de Spearman igual a 0.633 se entiende como el eficiente rango para el Proceso en Digitalización de documentos está correspondido con nivel de alto para Seguridad en la información de la Secretaría General de un Centro Superior Universitario; al nivel ineficiente del Proceso para la Digitalización de documentación tiene correspondencia con el bajo nivel en Seguridad para la información de la Secretaría General de un Centro Superior Universitario.

En relación a ello, Urbina (2012) indico respecto a pasos para digitalizar documentación, que permite almacenar bajo la manera resistente esa retrato del manuscrito originalmente lo cual permitirá la proyección de la imagen y reproducción de dicha imagen en copias en papel, para ello se emitieron reglas metodológicas en cuanto a seguridad para permiten tener la certeza de que la información no será alterada.

Por su parte, Olaza (2017) afirmó que; los proceso de digitalización de material bibliográfico se concentró en la aplicar tecnología informatizada para escanear esa que se encuentra plasmada físicamente, concluyendo que el recinto bibliotecario de la nación

cuenta con adelantos referidos al tema para digitalizar, que alcancen las características de conservar, integrar, controlar el acervo documentario, defender y difundir, para lo cual deben establecer estrategias que aseguren toda data orientadas en un aprovechamiento efectivo de los recursos además preservación digital de la información administrada, asegurando que los documentos estarán escaneados a la vez divulgados por medios virtuales, que abarquen masivamente esta comunicación la disposición para diferentes consultas.

Por otro lado, Yan y Zavala (2015) quienes tuvieron el propósito de la presentación planificada para mejoramiento en el aseguramiento de toda información, que haga referirse a las fortalezas tecnológicas para su protección con el propósito en que dicha data esté fortalecida de manera disponible, confidencial e íntegra, lo cual complementa lo afirmado por los anteriores autores, puesto que, un alto nivel de seguridad de información, que proteja entre otros a los equipos de hardware y licencias de software que forman parte de los procesos de digitalización de documentos permitirá que este sea eficiente.

Asimismo, Olaza (2017) manifestó que; la asegurar data viene a ser un proceso vital en el desarrollo y mantenimiento de una empresa, considerándose que día a día aumenta la información de la mano con su captura digitalmente, por tanto, se requieren vigilancias para garantizar adecuadamente el encontrarse disponible, íntegro y de manera confidencial la información, Puesto que, en los procesos de adquisiciones, interactúan con documentación física que es digitalizada, la cual es enviada y recibida por correo electrónico y sistema, razón por la cual se debe asegurar la inalterabilidad de esta, lo que se consigue con un eficiente proceso de digitalización, el cual permite un mayor rango para asegurar la data garantizando su integridad en el documento remitido.

Además, Rebollo (2014) testificó que; la captura de información es un procedimiento automatizado robusto dirigido en el guardar, consultas, la administración, presentado en formato digitalmente. Pues, la firma Digital, como paso final del proceso de digitalización, presentado como un instrumento que le de valor a la información digitalizada permitiendo cumplir con la funciones de seguridad de la información.

Igualmente, Williams (2015) señaló respecto al proceso de digitalización de documentos o migración en respaldo digitalmente, que presente variadas opciones de las mismas. Su finalidad para que el repositorio de historia no ocasione su maltrato al no tener acceso el empleo manualmente, lográndose disminuir tiempos y ser accesible amigablemente hacia la información; sería el recurso óptimo para mantener el formato físico de los repositorios documentales, permite el medio de acceder a la información por medios sistematizados, lo que facilita su consulta a los documentos desde diferentes ubicaciones geográficas, sin estar expuestos alguna amenaza de su contenido, dichos documentos no circulan sin control y permite un backup de la documentación.

Concordando plenamente con los resultados de la presente investigación donde se establece la interrelación de las variables de investigación.

Respecto a la hipótesis específica<sup>2</sup>; esta indica: Existe la relación entre el. Normativa para Digitalización de documentos y Seguridad en la información en la Secretaría general en un Centro Superior Universitario. Dicho supuesto obtiene valor al resultar el coeficiente para correlación Rho de Spearman igual a 0.471 se entiende como el eficiente rango para el Normativa en Digitalización de documentos está correspondido con nivel de alto para Seguridad en la información de la Secretaría General de un Centro Superior Universitario; al nivel ineficiente del Normativa para la Digitalización de documentación tiene correspondencia con el bajo nivel en Seguridad para la información de la Secretaría General de un Centro Superior Universitario.

En relación a ello, Urbina (2014) indicó; respecto la normativa, esta señala aspectos relacionados con la seguridad, particularmente, la Norma Técnica Peruana 392.030-2, establece procedimientos para otorgar valor legal a las micro formas, que por medio de fedatarios certifican la veracidad en las fotocopias virtuales y almacenadas en los medios no regrabables, y se almacenan en bóvedas, bajo ciertos criterios en la seguridad que se encuentran prescritas en las reglas, garantizando ser confidencial, ser íntegra, y estar disponible tal información, dimensiones corresponden a la data segura.

Además, Rebollo (2014) testificó que; la Ley N° 26612 altera ese D.Leg. Nro.681, el cual establecer como controlar la manipulación tecnológica de punta referidos a files documental, que reconoce el valor legal de los documentos digitalizados con intervención

de un fedatario (Digitalización con valor legal) o microformas serán transformados como respaldo legal, para tributos en su defecto de control interno para la organización, con lo cual genera reducción de costos en cuanto al impreso físicamente, y se prescribe que cualquier adulteración del documento digitalizado con valor legal (microforma), evita la comisión delincinencial contra el patrimonio en su modalidad de la fé pública, refuerza la relación que con una eficiente Normativa de la Digitalización de documentos corresponde un alto nivel de información segura.

Concordando plenamente con los resultados de la presente investigación donde se establece la interrelación con la normativa de las variables de investigación.

Respeto a la hipótesis específica<sup>3</sup>; esta indica: Existe la relación entre el. Soporte técnico para Digitalización de documentos y Seguridad en la información en la Secretaría general en un Centro Superior Universitario. Dicho supuesto obtiene valor al resultar el coeficiente para correlación Rho de Spearman igual a 0.720 se entiende como el eficiente rango para el Soporte técnico en Digitalización de documentos está correspondido con nivel de alto para Seguridad en la información de la Secretaría General de un Centro Superior Universitario; al nivel ineficiente del Soporte técnico para la Digitalización de documentación tiene correspondencia con el bajo nivel en Seguridad para la información de la Secretaría General de un Centro Superior Universitario.

En relación a ello, Urbina (2014) indico; para la alcanzar validar los equipos está en considerar medir cualitativa su uso, a fin de obtener una optimización en lo correspondiente a la seguridad, restando las probabilidades que signifique la alteración de un documento escaneado.

Por otra parte, Tola (2015) afirmó que; la calibración de equipos de digitalización con capacidad robusta asignado solo a esta actividad debido al requerimiento alto en el proceso de digitalización, que permitan contar con los equipos de creación y reproducción para que alcancen las características de conservar, integrar, controlar el acervo documentario, defender y difundir, para lo cual deben establecer estrategias que aseguren toda data orientadas en un aprovechamiento efectivo delos recursos además preservación digital de la información administrada, asegurando que los documentos estarán

escaneados a la vez divulgados por medios virtuales, que abarquen masivamente esta comunicación la disposición para diferentes consultas.

Asimismo, Olaza (2017) recomendó; establecer revisiones periódicas para el mantenimiento de los equipos, así como controla la accesibilidad hacia estos, pues esa mayor parte correspondiente a la data reside dentro de estos, conociendo que los equipos son activos críticos, se deberán de guardar bajo los niveles de seguridad suficientes, lo que permite un mayor nivel de seguridad de la información.

Además, Rebollo (2014) testificó que; esas peculiaridades que tienen los files proveen estar disponibles en un soporte que digitalice con parámetros, así como ejercicios determinados orientados para ejecutar la funciones que permitan asegurar la data.

Igualmente, Williams (2015) en su análisis de resultados obtenidos en su investigación; interpreto que el soporte tecnológico del Fondo Documental Belisario Porras era malo y la competencia del personal en tecnologías era regular, de ahí que, la seguridad de la información resulto de regular a mala, concluyendo que las nuevas tecnologías serán su mejor soporte, en la medida que se hayan adecuado a la digitalización de documentos para con ello mejorar la seguridad de la información del fondo.

Concordando plenamente con los resultados de la presente investigación sobre el soporte técnico donde se establece la interrelación de las variables de investigación.

## V. Conclusiones

**Primero.** Alcanzó a determina la relación entre Digitalización de documentos y la Seguridad de información en Secretaría General del un Centro Superior Universitario de Lima, habiéndose obtenido un p - valor (\*\* $p < 0.01$ ), es decir hay una correlación altamente significativa, es más, se calculó el indicador para la correlación en 0,785, representando alto correlación.

**Segunda** Se demuestra la interrelación con el Proceso de Digitalizar documentos y Seguridad de su información dentro de la Secretaría General, de un Centro Superior Universitario Lima, habiéndose obtenido un p - valor (\*\* $p < 0.01$ ), es decir hay una correlación altamente significativa, incluso, se calculó el indicador de relación en 0,733, representa el rango alto en su correlación, lo cual confirma la primera hipótesis específica de la investigación. Que señala rango eficiente en el Proceso del Digitalización de documentación tiene correspondencia con alto rango en la Seguridad para la información en la Secretaría General de un Centro Superior Universitario.

**Tercera** Se evidencia que existe relación directa entre la Normativa de la Digitalizar documentos y Seguridad en la información de Secretaría General en un Centro Superior Universitario Lima, habiéndose obtenido un p - valor (\*\* $p < 0.01$ ), es decir hay una correlación altamente significativa, asimismo, se calculó el coeficiente que estima su correlación en 0.471, representando el rango moderado en la correlación, lo cual confirma la segunda hipótesis específica de la investigación.

**Cuarto** Se evidenció la interrelación directa del Soporte técnico de la Digitalización de documentos con la Seguridad en la información de la Secretaría General, de un Centro Superior Universitario Lima, habiéndose obtenido un p - valor (\*\* $p < 0.01$ ), es decir hay una correlación altamente significativa, igualmente, se calculó el indicador correlacional en 0,720, significando representa el rango alto en la correlación, lo cual confirma la tercera hipótesis específica de la investigación.

## **VI. Recomendaciones**

- Primera** A la Secretaria General realice un proceso de fortalecimiento de las capacidades de digitalización de documentos en la entidad, dirigido a quienes participan en los procesos de digitalización, así como los trabajadores que forman parte de la elaboración de normativas y soporte técnico, para aumentar de manera eficiente la digitalización de los documentos para que de esa tal manera que incremente el nivel del aseguramiento.
- Segunda** Se recomienda que los empleados involucrados participan en los procesos de digitalización de documentos hagan llegar aportes con ideas inquietantes que permitan aportar para el fortalecimiento del procesamiento en digitalizar información, pasando la valla de debilidad y así lograr la toma de decisiones adecuadas y que contribuirá a superar dicho nivel de seguridad.
- Tercera** También recomienda al departamento para Gestionar Procesos y Calidad, elaborar y mantener actualizada la normativa de digitalización de documentos, capaciten y sensibilicen al resto de la institución, sobre estas normas y su influencia en la de asegurar la data
- Cuarta** El departamento de Secretaría de General, que mantenga su visión para integrar en sus filas personales con formación en informática y carreras afines, con lo que se continuará con la mejora continua del soporte técnico de la digitalizar documentación de mano con mantenerlo seguro.

## Referencias

- Sampedro Guamán, C. R., Machuca Vivar, S. A., Palma Rivera, D. P., & Carrera Calderón, F. A. (2019). Percepción De Seguridad De La Información en Las Pequeñas Y Medianas Empresas en Santo Domingo. *Investigación Operacional*, 40(3), 421–428. Retrieved from <http://search.ebscohost.com/login.aspx?direct=true&db=a9h&AN=136929577&lang=es&site=ehost-live>
- Marchisotti, G. G., Joia, L. A., & De Carvalho, R. B. (2019). The Social Representation of Cloud Computing According to Brazilian Information Technology Professionals. *RAE: Revista de Administração de Empresas*, 59(1), 16–28. <https://doi.org/10.1590/S0034-759020190103>
- Benavides Sepúlveda, A., & Blandón Jaramillo, C. (2018). Modelo sistema de gestión de seguridad de la información para instituciones educativas de nivel básico. *Scientia et Technica*, 23(1), 85–92. Retrieved from <http://search.ebscohost.com/login.aspx?direct=true&db=a9h&AN=130405186&lang=es&site=ehost-live>
- Parada, D. J., Flórez, A., & Gómez, U. E. (2018). Analysis of the Components of Security from a Systemic System Dynamics Perspective. *Información Tecnológica*, 29(1), 27–38. <https://doi.org/10.4067/S0718-07642018000100027>
- Lo Giudice, M. E. (2017). Business data, its protection in the current knowledge society: an argentine perspective. *Revista de Derecho Comunicaciones y Nuevas Tecnologías*, (17), 1–20. <https://doi.org/10.15425/redecom.17.2017.06>
- López Echeverry, A. M., & Villa Sánchez, P. A. (2016). Política de gestión de contraseñas para usuarios finales. *Scientia et Technica*, 21(2), 128–134. Retrieved from <http://search.ebscohost.com/login.aspx?direct=true&db=a9h&AN=122337585&lang=es&site=ehost-live>
- García-Morales, E. (2016). Riesgos y seguridad de la información: convergencias desde la gestión documental. *Anuario Think EPI*, 10, 131–133. <https://doi.org/10.3145/thinkepi.2016.27>
- Angarita, A. A., Tabares, C. A., & Rios, J. I. (2015). Definition of a model for measuring risk analysis of security information applying fuzzy logic and systems based on knowledge, 9(17), 71–80. Retrieved from <http://search.ebscohost.com/login.aspx?direct=true&db=a9h&AN=109152575&lang=es&site=ehost-live>

Wipo Publishes Patent Of Nec For "Security Information Analysis Device, Security Information Analysis Method, Security Information Analysis Program, Security Information Evaluation Device, Security Information Evaluation Method, Security Information Analysis System And Recording Medium" (Japanese Inventor). (2018, Aug 06). *US Fed News Service, Including US State News* Retrieved from <https://search.proquest.com/docview/2083851019?accountid=37408>

Information security forum: All rise - the ISF defines the changing role of information security in the enterprise; information security forum lays out vision for information security and says information security professionals want to play a more integrated and pro-active role in business. (2008, Jul 28). *M2 Presswire* Retrieved from <https://search.proquest.com/docview/444413676?accountid=37408>

Information security; data on information security described by researchers at university of sistan and baluchestan (the impact of the security competency on "self-efficacy in information security" for effective health information security in iran). (2016, Nov 01). *Information Technology Newsweekly* Retrieved from <https://search.proquest.com/docview/1832810972?accountid=37408>

US patent issued to konica minolta on july 2 for "security information update system, information processing apparatus, security information update method and non-transitory computer-readable recording medium encoded with security information update program" (japanese inventor). (2019, Jul 03). *US Fed News Service, Including US State News* Retrieved from <https://search.proquest.com/docview/2250654818?accountid=37408>

Konica minolta (4902) issued patent titled "security information update system, information processing apparatus, security information update method and non-transitory computer-readable recording medium encoded with security information update program". (2019, Jul 05). *News Bites - Electronics* Retrieved from <https://search.proquest.com/docview/2251782109?accountid=37408>

Information technology - information security; new information security study results from university of tehran described (HPCgnature: A hardware-based application-level intrusion detection system). (2019, Feb 05). *Information Technology Newsweekly* Retrieved from <https://search.proquest.com/docview/2176574777?accountid=37408>

- Technical support services for the subsystem for collecting and analyzing information security information security events for the information systems of the central office of belagroprombank ojsc 1 const. (2018). *MENA Report*, Retrieved from <https://search.proquest.com/docview/2125979124?accountid=37408>
- Barnard, A. (2011). *Archivos electrónicos. Textos y Contextos*. Puebla: Benemérita Universidad Autónoma de Puebla.
- Bernal, C. (2006). *Metodología de la investigación*. México: Pearson educación.
- Bisquerra, R. (2009). *Metodología de la investigación educativa*. Madrid: Muralla.
- Cano, J. (2011). *La Gerencia de la Seguridad de la Información: Evolución y Retos Emergentes*. ISACA JOURNAL.
- Carvajal, A. (2002). *Teorías y Modelos: Formas de representación de la realidad*. Cartago: Instituto Tecnológico de Costa Rica.
- Cuevas, G. (1975). *Teoría de la información, codificación y lenguajes*. Argentina: Ministerio de Educación.
- Días, N. (2013). *Aplicación de TICS en la conservación y difusión de patrimonio documental y bibliográfico, en la Biblioteca Nacional del Perú*. (Tesis de maestría, Universidad de Piura, Piura). Recuperada de <https://pirhua.udep.edu.pe/handle/11042/1804>
- Dirección general para el impulso de la administración electrónica. (2011). *Guía de aplicación de la norma técnica de interoperabilidad*. Madrid: Ministerio de Política Territorial y Administración Pública.
- Frayssinet, M. (2014). *Taller de Implementación de la norma ISO 27001*. Lima: ONGEI.
- Fuster, F. (1999). *Archivística, Archivo, Documento de Archivo*. Universidad de Murcia.
- Galindo, C. (2014). *Seguridad de la Información: Revista de la Segunda Cohorte del Doctorado en Seguridad Estratégica*. Guatemala: Universidad San Carlos de Guatemala.
- García, F. (2006). *El Cuestionario: Recomendaciones metodológicas para el diseño*. Mexico DF: Editorial Limusa.
- Gonzales, J. (2011). *¿Seguridad Informática o Seguridad de la Información?* España: [www.seguridadparatodos.es](http://www.seguridadparatodos.es).
- Hernández Sampieri, R. (2010). *Metodología de la Investigación*. México: McGraw-Hill.
- Iberico, L. (2013). *Mejoramiento de la gestión de trámite documentario utilizando firma digital en el proyecto especial alto mayo - moyobamba ed . moyobamba: universidad nacional de san martín*.

- Infante, D. (2011). *Digitalización y gestión documental*. Lima: ONGEI.
- Instituto Nacional de Defensa de la Competencia y de la Protección de la Propiedad Intelectual. (2007). NTP- ISO/IEC 17799. Recuperado de <https://delgadocaramutti.files.wordpress.com/2010/06/ntp1.pdf>
- Instituto Nacional de Defensa de la Competencia y de la Protección de la Propiedad Intelectual. (2014). NTP- ISO/IEC 27001. Recuperado de [https://www.google.com.pe/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&cad=rja&uact=8&ved=0ahUKEwieqP\\_i6N\\_XAhUGDZAKHTOJDKUQFggkMAA&url=https%3A%2F%2Fcanvas.utp.edu.pe%2Fcourses%2F8870%2Ffiles%2F42244%2Fdownload%3Fdownload\\_frd%3D1&usg=AOvVaw1HgEedCZ4xpVOVhlw77odi](https://www.google.com.pe/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&cad=rja&uact=8&ved=0ahUKEwieqP_i6N_XAhUGDZAKHTOJDKUQFggkMAA&url=https%3A%2F%2Fcanvas.utp.edu.pe%2Fcourses%2F8870%2Ffiles%2F42244%2Fdownload%3Fdownload_frd%3D1&usg=AOvVaw1HgEedCZ4xpVOVhlw77odi)
- Instituto Nacional de Calidad. (2015). NTP- ISO/IEC 392.030-2. Recuperado de <https://ismaelgonzalezotoyablog.files.wordpress.com/2016/06/enviando-ntp392-030-2.pdf>
- Lampreabe, B. (2008). *Metodología de Digitalización de Documentos*. España: EJE S.A.
- Norma técnica peruana 392.030-2. (2015). Lima: INACAL.
- Robles, L. (2012). *Modelos de seguridad de la información*. Panamá: Universidad Latina.
- Rodriguez, G. (2012). *Sistema de Producción de Microformas*. Lima: Secretaría General de un Centro Superior Universitario.
- Sánchez, H., & Reyes, C. (2006). *Metodología y diseños en la investigación*. Lima: Visión Universitaria.
- Soto, R. I. (2015). *La tesis de maestría y doctorado en 4 pasos 2da edición*. Lima: Colección Nuevo Milenio.
- Suarez, G. (2013). *Estudio de la Seguridad de la Información aplicado a Recursos Humanos, Adquisiciones y Cómputo para empresas del Sector Pesquero*. (Tesis de maestría, Universidad de Guayaquil, Ecuador). Recuperada de <http://repositorio.ug.edu.ec/handle/redug/257>
- Tamayo y Tamayo, M. (2004). *Proceso de la Investigación Científica*. Mexico: Limusa.
- Urbina, C. (2012). *Certificación para la digitalización de documentos en Chile*. (Tesis de maestría, Universidad de Chile, Chile). Recuperada de <http://repositorio.uchile.cl/handle/2250/104416>

- Valderrama, S. (2013). *Pasos para elaborar proyectos de Investigación Científica*. Lima: San Marcos.
- Vázquez de Parga, M. (2016). *Digitalizar ¿Para qué? Principios y criterios a tener en cuenta en los proyectos de digitalización del patrimonio documental*. Lima: Archivo General de la Nación Perú.
- Vega, J. A. (2014). *El documento jurídico y su electrificación*. Madrid: Editorial Reus.
- Vinuesa, L. (2005). La encuesta. Observación extensiva de la realidad social. En R. Berganza, & J. Ruiz, *Investigar en comunicación*. Madrid: McGraw-Hill Interamericana.
- Voutssas-M, J., & Barnard, A. (2014). *Glosario de Preservación Archivística Digital*. México: Universidad Nacional Autónoma de México.
- Williams, E. L. (2010). *Propuesta para la Digitalización del Fondo documental del DR. Belisario Porras*. (Tesis de maestría, Universidad Internacional de Andalucía, España). Recuperada de <http://dspace.unia.es/handle/10334/1789>
- Yan, F., & Zavala, C. (2013). *Plan de mejora de la Seguridad de Información y Continuidad del Centro de Datos de la Gerencia Regional de Educación La Libertad aplicando lineamientos ISO 27001 y buenas prácticas COBIT*. (Tesis de maestría, Universidad Privada Antenor Orrego, Trujillo). Recuperada de <http://repositorio.upao.edu.pe/handle/upaorep/53/simplesearch?query=645>
- Yuni, J., & Urbano, C. (2006). *Técnicas para investigar: recursos metodológico"para la preparación de proyectos de investigación*. Córdoba: Brujas.

[http://repositorio.ucv.edu.pe/bitstream/handle/UCV/18463/Maldonado\\_EEE.pdf?sequence=1&isAllowed=y](http://repositorio.ucv.edu.pe/bitstream/handle/UCV/18463/Maldonado_EEE.pdf?sequence=1&isAllowed=y)

<http://www.dspace.espol.edu.ec/xmlui/bitstream/handle/123456789/31114/Resumen%20de%20tesis%20Tola%2c%20director%20de%20tesis%20Msig.%20Lenin%20Freire%20C.%2019%20mayo%202015.pdf?sequence=1&isAllowed=y>

**ANEXOS**

**Anexo 01: Consentimiento**



UNIVERSIDAD CÉSAR VALLEJO

“AÑO DE LA LUCHA CONTRA LA CORRUPCIÓN Y LA IMPUNIDAD”

Lima, 4 de abril de 2019

**OFICIO N° 0226-2019/SG-UCV**

**Dr. CARLOS VENTURO ORBEGOSO**  
Jefe de la Escuela de Posgrado filial LimaNorte

**ASUNTO:** Facilidades para trabajo de investigación

Es grato dirigirme a usted para expresarle mi saludo y a la vez informarle que ha solicitud del Ing. Marco Antonio Soto Martínez, Coordinador de Secretaria General y estudiante del Programa de Maestría en Ingeniería de Sistemas con mención en Tecnologías de la Información de la Escuela de Posgrado, se le otorgo las facilidades para la realización de su trabajo de investigación así como aplicación de encuestas como parte de dicho proceso.

Sin otro particular, es propicia la oportunidad para expresarle los sentimientos de mi especial consideración.

Atentamente,



*Victor Rafael Santisteban Chávez*  
Ing. Victor Rafael Santisteban Chávez  
SECRETARIO GENERAL

**Anexo 02:**  
**Operacionalización de las variables/Matriz de Consistencia**

Cuadro de operacionalización de la variable1

*Digitalización de documentos*

<b>Dimensiones</b>	<b>Indicadores</b>	<b>Ítems</b>	<b>Escalas</b>	<b>Niveles y Rango</b>
	Documentos recibidos	1-2		
Proceso	Cantidad de imágenes generadas	3		Eficiente
	Documentos digitalizados	4-10	1 = Nunca	(74-100)
			2 = Casi nunca	Poco eficiente
Normativa	Normas legales cumplidas	11	3 = A veces	(47-73)
	Normas técnicas cumplidas	12-13	4 = Casi siempre	Ineficiente
			5 = Siempre	(20-46)
Soporte técnico	Equipos de hardware requeridos	14-17		
	Licencias de software requeridos	18-20		

Fuente: Elaboración propia.

Operacionalización de la variable 2:

*Seguridad de la información*

<b>Dimensiones</b>	<b>Indicadores</b>	<b>Ítems</b>	<b>Escalas</b>	<b>Niveles y Rango</b>
Confidencialidad	Accesos no autorizados	1-4		
	Configuración por defecto	5-7		
	Suplantación de IP o datos	8-9		
	Monitoreo no autorizado	10	1 = Nunca	Alto (70-95)
	Contraseñas débiles	11-12	2 = Casi nunca	Medio
Disponibilidad	Negación del servicio	13-14	3 = A veces	(44-69)
	Inundación de paquetes	15	4 = Casi siempre	Bajo
	Eliminar, borrar o manipular datos	16	5 = Siempre	(19-43)
	Seguridad física y ambiental	17		
Integridad	Eliminar, borrar o manipular datos	18-19		
	Virus informático	20		

Fuente: Elaboración propia

**Matriz de consistencia**

**Título: Digitalización de documentos y seguridad de la información en la Secretaría General de un Centro Superior Universitario, Lima Norte 2019**

**Autor: Bach. Marco Antonio Soto Martínez**

<b>Problema</b>	<b>Objetivos</b>	<b>Hipótesis</b>	<b>Variables e indicadores</b>				
<b>Problema General</b>	<b>Objetivo General</b>	<b>Hipótesis General</b>	<b>Variable 1: Digitalización de documentos</b>				
			<b>Dimensiones</b>	<b>Indicadores</b>	<b>Ítems</b>	<b>Escala de medición</b>	<b>Niveles y rangos</b>
¿Cuál es la relación entre Digitalización de Documentos y la Seguridad de la Información en la Secretaría General de un Centro Superior Universitario, Lima Norte, 2019?	Determinar la relación entre Digitalización de Documentos y la Seguridad de la Información en la Secretaría General de un Centro Superior Universitario, Lima Norte, 2019	la Existe una relación directa entre la Digitalización de Documentos y la Seguridad de la Información en la Secretaría General de un Centro Superior Universitario, Lima Norte, 2019		Documentos recibidos	1-2		
			Proceso	Cantidad de imágenes generadas	3	1 = Nunca 2 = Casi nunca 3 = A veces	Eficiente (74-100) Poco eficiente (47-73)
			Normativa	Documentos digitalizados	4-10	4 = Casi siempre	
				Normas legales cumplidas	11	5 = Siempre	Ineficiente (20-46)
				Normas técnicas cumplidas	12-13		

Hardware  
requerido 14-17

Soporte técnico  
Licencias de  
software 18-20  
requeridos

**Variable 2: Seguridad de la información**

<b>Problemas Específicos</b>	<b>Objetivos Específicos</b>	<b>Hipótesis Específicas</b>	<b>Dimensiones</b>	<b>Indicadores</b>	<b>Ítems</b>	<b>Escala de medición</b>	<b>Niveles y rangos</b>
¿Cuál es la relación entre la digitalización de documentos y la confidencialidad en la seguridad de la información en la Secretaría General de un Centro Superior Universitario, Lima Norte, 2019?	Determinar la relación entre la digitalización de documentos y la confidencialidad en la seguridad de la información en la Secretaría General de un Centro Superior Universitario, Lima Norte, 2019	la Existe una relación directa entre la digitalización de documentos y la confidencialidad en la seguridad de la información en la Secretaría General de un Centro Superior Universitario, Lima Norte, 2019	Confidencialidad	Accesos autorizados	no 1-4	1 = Nunca	Alto (70-95)
				Configuración por defecto	5-7		
¿Cuál es la relación entre la digitalización de documentos y la confidencialidad en la seguridad de la información en la Secretaría General de un Centro Superior Universitario, Lima Norte, 2019?	Determinar la relación entre la digitalización de documentos y la confidencialidad en la seguridad de la información en la Secretaría General de un Centro Superior Universitario, Lima Norte, 2019	la Existe una relación directa entre la digitalización de documentos y la confidencialidad en la seguridad de la información en la Secretaría General de un Centro Superior Universitario, Lima Norte, 2019	Disponibilidad	Suplantación de IP o datos	8-9	3 = A veces	Medio (44-69)
				Monitoreo autorizado	no 10	4 = Casi siempre	Bajo (19-43)
¿Cuál es la relación entre la digitalización de documentos y la confidencialidad en la seguridad de la información en la Secretaría General de un Centro Superior Universitario, Lima Norte, 2019?	Determinar la relación entre la digitalización de documentos y la confidencialidad en la seguridad de la información en la Secretaría General de un Centro Superior Universitario, Lima Norte, 2019	la Existe una relación directa entre la digitalización de documentos y la confidencialidad en la seguridad de la información en la Secretaría General de un Centro Superior Universitario, Lima Norte, 2019	Disponibilidad	Contraseñas débiles	11-12	5 = Siempre	
				Negación del servicio	del 13-14		

digitalización de documentos y la disponibilidad en la seguridad de la información en la Secretaría General de un Centro Superior Universitario, Lima Norte, 2019?

¿Cuál es la relación entre la digitalización de documentos y la integridad en la seguridad de la información en la Secretaría General de un Centro Superior Universitario, Lima Norte, 2019?

digitalización de documentos y la disponibilidad en la seguridad de la información en la Secretaría General de un Centro Superior Universitario, Lima Norte, 2019?

Determinar la relación entre la digitalización de documentos y la integridad en la seguridad de la información en la Secretaría General de un Centro Superior Universitario, Lima Norte, 2019

digitalización de documentos y la disponibilidad en la seguridad de la información en la Secretaría General de un Centro Superior Universitario, Lima Norte, 2019?

Existe una relación directa entre la digitalización de documentos y la integridad en la seguridad de la información en la Secretaría General de un Centro Superior Universitario, Lima Norte, 2019

Integridad

Inundación de paquetes 15

Eliminar, borrar o manipular datos 16

Seguridad física y ambiental 17

Eliminar, borrar o manipular datos 18-19

20

Virus informático

Tipo y diseño	Población y muestra	Técnicas e instrumentos	Estadística a utilizar
<p>Tipo: Básica  Alcance: Correlacional  Diseño: No experimental, transversal  Método: Hipotético deductivo</p>	<p>Población: Conformada por 20 trabajadores</p>	<p>Variable 1: Digitalización de documentos  Técnica: Encuesta  Instrumentos: Oral, escrita. Guía de encuesta  Autor: Marco Antonio Soto Martínez  Año: 2019  Monitoreo:  Ámbito de aplicación: Personal de grados y títulos, secretaría general, archivo central y repositorio  Forma de administración: Directa</p> <p>Variable 2: Seguridad de la información  Técnica: Encuesta  Instrumentos: Oral, escrita. Guía de encuesta  Autor: Marco Antonio Soto Martínez  Año: 2019  Monitoreo:  Ámbito de aplicación: Personal de grados y títulos, secretaría general, archivo central y repositorio  Forma de administración: Directa</p>	<p>DESCRIPTIVA: Se realizará la observación estadística de la colección de datos obtenidas con el instrumento con lo que se alimentará las tablas de frecuencia y porcentajes con sus respectivos gráficos expresados en porcentajes, utilizando SPSS v.25, terminando con el análisis interpretativo de los resultados.</p>
			<p>INFERENCIAL: Se aplicará la prueba de coeficiente de correlación para determinar si existe correlación (asociación o interdependencia) entre las dos variables con la “Prueba de Rho de Spearman”.</p>

---

**Anexo 03:**  
**Base de datos**

DIGITALIZACIÓN DE DOCUMENTOS																			
D1. Proceso										D2. Normativa					D3: Soporte Técnico				
P1	P2	P3	P4	P5	P6	P7	P8	P9	P10	P11	P12	P13	P14	P15	P16	P17	P18	P19	P20
3	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4
4	3	4	4	4	4	4	4	3	3	4	3	4	4	4	3	4	4	4	4
4	3	3	3	4	4	4	4	4	4	4	3	3	3	3	4	4	4	4	4
3	4	4	3	3	4	3	4	4	3	4	4	3	3	3	4	4	4	3	4
4	3	4	3	4	4	3	4	3	4	4	4	4	4	4	4	4	4	4	4
4	4	3	3	4	4	4	4	3	4	3	4	4	4	4	4	4	3	4	3
3	4	4	4	3	3	3	4	4	3	3	4	3	4	4	4	4	4	4	4
4	3	4	4	4	4	3	3	3	4	4	3	4	4	4	4	4	4	4	4
4	4	4	4	4	4	3	4	4	3	4	4	4	3	4	4	4	3	4	3
4	4	4	4	4	4	3	4	4	4	4	4	4	4	4	4	4	4	4	4
4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4
3	3	3	3	4	4	4	4	4	4	3	4	3	4	3	3	3	3	3	3
3	3	3	4	3	4	3	3	3	4	4	3	4	3	3	3	3	3	3	3
4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4
4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4
3	4	3	4	4	4	3	4	4	4	4	3	4	4	4	3	4	4	4	4
3	4	3	3	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4
3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3
4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4

SEGURIDAD DE LA INFORMACIÓN																			
D1. Confidencialidad										D2. Disponibilidad							D3: Integridad		
P1	P2	P3	P4	P5	P6	P7	P8	P9	P10	P11	P12	P13	P14	P15	P16	P17	P18	P19	P20
4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4
4	4	4	4	4	4	3	4	4	4	4	4	4	4	4	3	4	4	4	4
3	4	4	4	4	4	3	4	3	3	3	3	3	4	4	4	4	4	4	3
4	4	4	4	4	4	4	4	3	3	3	3	3	4	4	4	4	4	3	4
4	4	4	4	4	4	4	4	4	4	4	4	4	4	3	4	4	3	4	3
4	4	3	4	3	4	4	4	3	4	4	3	3	3	3	4	4	3	4	3
4	4	4	4	3	4	4	4	4	4	4	4	4	4	3	4	4	3	3	4
4	3	4	3	3	4	4	4	3	4	4	4	4	4	3	4	4	3	3	4
4	4	4	4	3	4	3	4	4	4	4	4	4	4	3	3	3	3	4	3
4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4
3	4	3	3	3	4	3	3	3	4	3	4	4	3	4	3	3	3	3	3
3	3	4	3	3	4	3	3	3	3	3	4	4	4	4	3	3	3	3	3
4	4	4	4	4	4	4	4	4	4	4	4	4	3	4	3	4	4	4	4
4	4	4	4	4	4	4	4	4	4	3	4	4	4	4	3	4	4	4	4
4	4	4	4	4	4	4	4	3	4	4	4	4	3	3	3	4	3	3	4
4	4	3	4	4	4	3	4	4	4	3	3	3	4	4	3	4	4	4	4
4	4	4	3	4	4	4	4	4	4	3	3	3	3	3	4	4	4	4	4
3	4	3	4	3	3	3	3	3	3	4	4	4	3	4	3	3	3	3	3
4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4
4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4
3	4	3	4	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3
4	4	4	4	4	4	4	3	4	4	4	4	4	4	4	4	4	4	4	4

**Anexo No.04. Instrumento**

## Instrumento de recolección de datos

### Cuestionario para medir la digitalización de documentos

#### I. Introducción

Estimado informante el presente documento tiene el objeto de conocer su opinión sobre el proceso de Digitalización de Documentos. Dicha información es completamente anónima y confidencial, por lo que solicito responder las interrogantes con sinceridad, y de acuerdo a su propia expectativa.

#### II. Indicaciones

A continuación se le presenta una serie de preguntas las cuales deberá responder marcando con una (X) la respuesta que considera pertinente y de acuerdo a escala, solo debes marcar una opción.

A	Nunca	1
B	Casi nunca	2
C	A veces	3
D	Casi siempre	4
E	Siempre	5

#### Variable: DIGITALIZACIÓN DE DOCUMENTOS

DIMENSIÓN	ÍTEMS	APRECIACIÓN				
		1	2	3	4	5
Proceso	1. Considera Ud., en que la entidad posee un cuadro de clasificación de documentos.					
	2. Considera Ud., que cuenta con ambientes adecuados para la conservación de documentos físicos recibidos para su preparación previa a su digitalización.					
	3. Considera Ud., que son adecuados los formatos a utilizar para los diversos tipos de documentos.					
	4. Considera Ud., que el documento digitalizado cuenta con la integridad y legibilidad suficiente					
	5. Considera Ud., que siempre debe llevarse una Clasificación de los documentos originales de acuerdo con los problemas de digitalización que se presenten.					
	6. Considera Ud., que es adecuado el tiempo requerido para la digitalización de documentos.					
	7. Considera Ud., que los documentos digitalizados poseen cualidades de durabilidad, inalterabilidad y fijeza similares a los documentos originales					
	8. Considera Ud., que los documentos digitalizados se encuentran accesibles.					
	9. Considera Ud., en que el acceso a la información conservada en discos ópticos supone que permanecerá legible, inteligible y recuperable.					
	10. Considera Ud., adecuado los controles empleados para archivar los documentos digitalizados.					

Normativa	11. Considera Ud., en que la intervención de un Fedatario Informático otorga valor legal al documento digitalizado.					
	12. Considera Ud., en que se debe cumplir con la normativa que establece hacer una auditoría una vez al año.					
	13. Considera Ud., que la organización debe contar con un programa de auditoría informática aplicable al sistema de digitalización.					
Soporte técnico	14. Considera Ud., que se cuenta con los equipos de hardware adecuados para el trabajo de digitalización.					
	15. Considera Ud., que los equipos de hardware (scáner) cuentan con los estándares de calibración para el trabajo de digitalización.					
	16. Considera Ud., en que la arquitectura del sistema de digitalización mejora los componentes del sistema sin degradar sus funciones y sin perder información.					
	17. Considera Ud., que el soporte de almacenamiento (Disco Externo NAS) se conserva en condiciones ambientales adecuadas.					
	18. Considera Ud., que los softwars requeridos en la digitalización cuentan con licencia					
	19. Considera Ud., en que el sistema puede acceder a la información ya digitalizada y convertirla a la nueva versión, permitiendo la transferencia de la información sin que sufra ninguna modificación.					
	20. Considera Ud., que se tiene la documentación técnica relacionada con la Seguridad de la información en todos los componentes del sistema de digitalización debidamente conservada.					

## Cuestionario para medir la seguridad de la información

### I. Introducción

Estimado informante el presente documento tiene el objeto de conocer su opinión sobre la Seguridad de la información. Dicha información es completamente anónima y confidencial, por lo que solicito responder las interrogantes con sinceridad, y de acuerdo a su propia expectativa.

### II. Indicaciones

A continuación se le presenta una serie de preguntas las cuales deberá responder marcando con una (X) la respuesta que considera pertinente y de acuerdo a escala, solo debes marcar una opción.

A	Nunca	1
B	Casi nunca	2
C	A veces	3
D	Casi siempre	4
E	Siempre	5

#### VARIABLE: Seguridad de la Información

DIMENSION	ITEMS	APRECIACION				
		1	2	3	4	5
Confidencialidad	1. Considera Ud., en que los usuarios cuentan con acceso a los servicios que han sido específicamente autorizados a usar.					
	2. Considera Ud., en que el acceso a la información y a las funciones del sistema están restringidas en concordancia con la política de control de acceso.					
	3. Considera Ud., que se tiene un adecuado Inventario de accesos a los sistemas.					
	4. Considera Ud., que los propietarios de los activos revisan los derechos de acceso de usuario en intervalos regulares.					
	5. Considera Ud., que se cuenta con la configuración por defecto para el hardware y software de digitalización.					
	6. Considera Ud., que se hacen efectiva las políticas de administración de configuraciones y actualizaciones de los sistemas operativos.					
	7. Considera Ud., que se requieren de cuentas usuarios genéricos o por defecto para la operación de los sistemas					

	8. Considera Ud., que es adecuado el sistema de inventarios de los equipos de red.					
	9. Considera Ud., que los usuarios deben contar con un conocimiento adecuado sobre el Spoofing					
	10. Considera Ud., en que se cuenta con una política de control de acceso documentada y revisada basada en los requisitos de negocio y seguridad de la información.					
	11. Considera Ud., que debe contarse con una gestión de contraseñas que aseguran la calidad de las mismas.					
	12. Considera Ud., que se realiza el cambio de contraseña cada cierto tiempo.					
Disponibilidad	13. Considera Ud, que se realiza la verificación, revisión y evaluación de los controles de continuidad de seguridad de la información a intervalos regulares					
	14. Considera Ud., en que las instalaciones de procesamiento de la información deben implementarse con redundancia suficiente para cumplir con requisitos de disponibilidad.					
	15. Considera Ud., que debe estar implementado y documentado procesos, procedimiento y controles para asegurar la continuidad de seguridad de la información.					
	16. Considera Ud., que se debe contar con metodologías de respaldo de información eficientes.					
	17. Considera Ud., en que la protección de los equipos contra fallas de electricidad aseguran la disponibilidad de los sistemas de información.					
Integridad	18. Considera Ud., que debe realizarse periódicamente respaldos de información.					
	19. Considera Ud., que la manipulación de datos debe ser realizado sin la alteración de los mismos.					
	20. Considera Ud., que el antivirus instalado en su equipo debe encontrarse correctamente actualizado y lo proteja tanto de virus como de otras amenazas informáticas.					

**Anexo No.05.**  
**Captura de pantalla resultados prueba de hipótesis**





## **Anexo No.06. Validación del Instrumento**

**CERTIFICADO DE VALIDEZ DE CONTENIDO DEL INSTRUMENTO QUE MIDE LA VARIABLE:  
DIGITALIZACIÓN DE DOCUMENTOS**

DIMENSIÓN	Pertinencia <sup>1</sup>		Relevancia <sup>2</sup>		Claridad <sup>3</sup>		Sugerencias
	Si	No	Si	No	Si	No	
<b>PROCESO</b>							
1. Considera Ud., en que la entidad posee un cuadro de clasificación de documentos.	X		X		X		
2. Considera Ud., que cuenta con ambientes adecuados para la conservación de documentos físicos recibidos para su preparación previa a su digitalización.	X		X		X		
3. Considera Ud., que son adecuados los formatos a utilizar para los diversos tipos de documentos.	X		X		X		
4. Considera Ud., que el documento digitalizado cuenta con la integridad y legibilidad suficiente	X		X		X		
5. Considera Ud., que siempre debe llevarse una Clasificación de los documentos originales de acuerdo con los problemas de digitalización que se presenten.	X		X		X		
6. Considera Ud., que es adecuado el tiempo requerido para la digitalización de documentos.	X		X		X		
7. Considera Ud., que los documentos digitalizados poseen cualidades de durabilidad, inalterabilidad y fijeza similares a los documentos originales	X		X		X		
8. Considera Ud., que los documentos digitalizados se encuentran accesibles.	X		X		X		
9. Considera Ud., en que el acceso a la información conservada en discos ópticos supone que permanecerá legible, inteligible y recuperable.	X		X		X		
10. Considera Ud., adecuado los controles empleados para archivar los documentos digitalizados.	X		X		X		
<b>NORMATIVA</b>							
11. Considera Ud., en que la intervención de un Fedatario Informático otorga valor legal al documento digitalizado.	X		X		X		
12. Considera Ud., en que se debe cumplir con la normativa que establece hacer una auditoria una vez al año.	X		X		X		
13. Considera Ud., que la organización debe contar con un programa de auditoría informática aplicable al sistema de digitalización.	X		X		X		
<b>SOPORTE TÉCNICO</b>							
14. Considera Ud., que se cuenta con los equipos de hardware adecuados para el trabajo de digitalización.	X		X		X		
15. Considera Ud., que los equipos de hardware (scáner) cuentan con los estándares de calibración para el trabajo de digitalización.	X		X		X		
16. Considera Ud., en que la arquitectura del sistema de digitalización mejora los componentes del sistema sin degradar sus funciones y sin perder información.	X		X		X		

17. Considera Ud., que el soporte de almacenamiento (Disco Externo NAS) se conserva en condiciones ambientales adecuadas.	X		X		X		
18. Considera Ud., que los softwars requeridos en la digitalización cuentan con licencia	X		X		X		
19. Considera Ud., en que el sistema puede acceder a la información ya digitalizada y convertirla a la nueva versión, permitiendo la transferencia de la información sin que sufra ninguna modificación.	X		X		X		
20. Considera Ud., que se tiene la documentación técnica relacionada con la Seguridad de la información en todos los componentes del sistema de digitalización debidamente conservada.	X		X		X		

**Observaciones (precisar si hay suficiencia): Existe suficiencia para su aplicación**

**Opinión de aplicabilidad:** Aplicable [ X ] Aplicable después de corregir [ ] No aplicable [ ]

**Apellidos y nombres del juez validador. Dr/ Mg: MG. TORRES CABANILLAS LUIS.**  
**DNI:08404690**

**Especialidad del validador: ING. ESTADISTICO CIP 49863**

**Lima, 20 de Abril del 2019**

<sup>1</sup>**Pertinencia:** El ítem corresponde al concepto teórico formulado.

<sup>2</sup>**Relevancia:** El ítem es apropiado para representar al componente o dimensión específica del constructo

<sup>3</sup>**Claridad:** Se entiende sin dificultad alguna el enunciado del ítem, es conciso, exacto y directo

**Nota:** Suficiencia, se dice suficiencia cuando los ítems planteados son suficientes para medir la dimensión

**Firma del Experto Informante**

**CERTIFICADO DE VALIDEZ DE CONTENIDO DEL INSTRUMENTO QUE MIDE LA VARIABLE:  
SEGURIDAD DE LA INFORMACIÓN**

DIMENSIÓN	Pertinencia <sup>1</sup>		Relevancia <sup>2</sup>		Claridad <sup>3</sup>		Sugerencias
	Si	No	Si	No	Si	No	
<b>CONFIDENCIALIDAD</b>							
1. Considera Ud., en que los usuarios cuentan con acceso a los servicios que han sido específicamente autorizados a usar.	X		X		X		
2. Considera Ud., en que el acceso a la información y a las funciones del sistema están restringidas en concordancia con la política de control de acceso.	X		X		X		
3. Considera Ud., que se tiene un adecuado inventario de accesos a los sistemas.	X		X		X		
4. Considera Ud., que los propietarios de los activos revisan los derechos de acceso de usuario en intervalos regulares.	X		X		X		
5. Considera Ud., que se cuenta con la configuración por defecto para el hardware y software de digitalización.	X		X		X		
6. Considera Ud., que se hacen efectiva las políticas de administración de configuraciones y actualizaciones de los sistemas operativos.	X		X		X		
7. Considera Ud., que se requieren de cuentas usuarios genéricos o por defecto para la operación de los sistemas	X		X		X		
8. Considera Ud., que es adecuado el sistema de inventarios de los equipos de red.	X		X		X		
9. Considera Ud., que los usuarios deben contar con un conocimiento adecuado sobre el Spoofing	X		X		X		
10. Considera Ud., en que se cuenta con una política de control de acceso documentada y revisada basada en los requisitos de negocio y seguridad de la información.	X		X		X		
11. Considera Ud., que debe contarse con una gestión de contraseñas que aseguran la calidad de las mismas.	X		X		X		
12. Considera Ud., que se realiza el cambio de contraseña cada cierto tiempo.	X		X		X		
<b>DISPONIBILIDAD</b>							
13. Considera Ud., que se realiza la verificación, revisión y evaluación de los controles de continuidad de seguridad de la información a intervalos regulares	X		X		X		
14. Considera Ud., en que las instalaciones de procesamiento de la información deben implementarse con	X		X		X		

redundancia suficiente para cumplir con requisitos de disponibilidad.	X		X		X		
15. Considera Ud., que debe estar implementado y documentado procesos, procedimiento y controles para asegurar la continuidad de seguridad de la información.	X		X		X		
16. Considera Ud., que se debe contar con metodologías de respaldo de información eficientes.	X		X		X		
17. Considera Ud., en que la protección de los equipos contra fallas de electricidad aseguran la disponibilidad de los sistemas de información.	X		X		X		
<b>INTEGRIDAD</b>							
18. Considera Ud., que debe realizarse periódicamente respaldos de información.	X		X		X		
19. Considera Ud., que la manipulación de datos debe ser realizado sin la alteración de los mismos.	X		X		X		
20. Considera Ud., que el antivirus instalado en su equipo debe encontrarse correctamente actualizado y lo proteja tanto de virus como de otras amenazas informáticas.	X		X		X		

**Observaciones (precisar si hay suficiencia):** Existe suficiencia para su aplicación

**Opinión de aplicabilidad:** Aplicable [ X ] Aplicable después de corregir [ ] No aplicable [ ]

**Apellidos y nombres del juez validador, Dr/ Mg:** MG. TORRES CABANILLAS LUIS.

**DNI:**08404690

**Especialidad del validador:** ING. ESTADISTICO CIP 49863

Lima, 20 de Abril del 2019

<sup>1</sup>**Pertinencia:** El ítem corresponde al concepto teórico formulado.

<sup>2</sup>**Relevancia:** El ítem es apropiado para representar al componente o dimensión específica del constructo

<sup>3</sup>**Claridad:** Se entiende sin dificultad alguna el enunciado del ítem, es conciso, exacto y directo

**Nota:** Suficiencia, se dice suficiencia cuando los ítems planteados son suficientes para medir la dimensión

Firma del Experto Informante

**CERTIFICADO DE VALIDEZ DE CONTENIDO DEL INSTRUMENTO QUE MIDE LA VARIABLE:  
DIGITALIZACIÓN DE DOCUMENTOS**

DIMENSIÓN	Pertinencia <sup>1</sup>		Relevancia <sup>2</sup>		Claridad <sup>3</sup>		Sugerencias
	Si	No	Si	No	Si	No	
<b>PROCESO</b>							
1. Considera Ud., en que la entidad posee un cuadro de clasificación de documentos.	X		X		X		
2. Considera Ud., que cuenta con ambientes adecuados para la conservación de documentos físicos recibidos para su preparación previa a su digitalización.	X		X		X		
3. Considera Ud., que son adecuados los formatos a utilizar para los diversos tipos de documentos.	X		X		X		
4. Considera Ud., que el documento digitalizado cuenta con la integridad y legibilidad suficiente	X		X		X		
5. Considera Ud., que siempre debe llevarse una Clasificación de los documentos originales de acuerdo con los problemas de digitalización que se presenten.	X		X		X		
6. Considera Ud., que es adecuado el tiempo requerido para la digitalización de documentos.	X		X		X		
7. Considera Ud., que los documentos digitalizados poseen cualidades de durabilidad, inalterabilidad y firmeza similares a los documentos originales	X		X		X		
8. Considera Ud., que los documentos digitalizados se encuentran accesibles.	X		X		X		
9. Considera Ud., en que el acceso a la información conservada en discos ópticos supone que permanecerá legible, inteligible y recuperable.	X		X		X		
10. Considera Ud., adecuado los controles empleados para archivar los documentos digitalizados.	X		X		X		
<b>NORMATIVA</b>							
11. Considera Ud., en que la intervención de un Fedatario Informático otorga valor legal al documento digitalizado.	X		X		X		
12. Considera Ud., en que se debe cumplir con la normativa que establece hacer una auditoría una vez al año.	X		X		X		
13. Considera Ud., que la organización debe contar con un programa de auditoría informática aplicable al sistema de digitalización.	X		X		X		
<b>SOPORTE TÉCNICO</b>							
14. Considera Ud., que se cuenta con los equipos de hardware adecuados para el trabajo de digitalización.	X		X		X		
15. Considera Ud., que los equipos de hardware (scáner) cuentan con los estándares de calibración para el trabajo de digitalización.	X		X		X		
16. Considera Ud., en que la arquitectura del sistema de digitalización mejora los componentes del sistema sin degradar sus funciones y sin perder información.	X		X		X		

17. Considera Ud., que el soporte de almacenamiento (Disco Externo NAS) se conserva en condiciones ambientales adecuadas.	X		X		X		
18. Considera Ud., que los softwares requeridos en la digitalización cuentan con licencia	X		X		X		
19. Considera Ud., en que el sistema puede acceder a la información ya digitalizada y convertirla a la nueva versión, permitiendo la transferencia de la información sin que sufra ninguna modificación.	X		X		X		
20. Considera Ud., que se tiene la documentación técnica relacionada con la Seguridad de la información en todos los componentes del sistema de digitalización debidamente conservada.	X		X		X		

**Observaciones (precisar si hay suficiencia):** Existe suficiencia para su aplicación

**Opinión de aplicabilidad:** Aplicable [ X ] Aplicable después de corregir [ ] No aplicable [ ]

**Apellidos y nombres del juez validador:** *Ms. Poletti Gaitán, Eduardo Humberto*  
*DNI. 18073124*

**Especialidad del validador:** *Docente Investigador*

Lima, 20 de Abril del 2019

<sup>1</sup>**Pertinencia:** El ítem corresponde al concepto teórico formulado.

<sup>2</sup>**Relevancia:** El ítem es apropiado para representar al componente o dimensión específica del constructo

<sup>3</sup>**Claridad:** Se entiende sin dificultad alguna el enunciado del ítem, es conciso, exacto y directo

**Nota:** Suficiencia, se dice suficiencia cuando los ítems planteados son suficientes para medir la dimensión



Firma del Experto Informante

**CERTIFICADO DE VALIDEZ DE CONTENIDO DEL INSTRUMENTO QUE MIDE LA VARIABLE:  
SEGURIDAD DE LA INFORMACIÓN**

DIMENSIÓN	Pertinencia <sup>1</sup>		Relevancia <sup>2</sup>		Claridad <sup>3</sup>		Sugerencias
	Si	No	Si	No	Si	No	
<b>CONFIDENCIALIDAD</b>							
1. Considera Ud., en que los usuarios cuentan con acceso a los servicios que han sido específicamente autorizados a usar.	X		X		X		
2. Considera Ud., en que el acceso a la información y a las funciones del sistema están restringidas en concordancia con la política de control de acceso.	X		X		X		
3. Considera Ud., que se tiene un adecuado inventario de accesos a los sistemas.	X		X		X		
4. Considera Ud., que los propietarios de los activos revisan los derechos de acceso de usuario en intervalos regulares.	X		X		X		
5. Considera Ud., que se cuenta con la configuración por defecto para el hardware y software de digitalización.	X		X		X		
6. Considera Ud., que se hacen efectiva las políticas de administración de configuraciones y actualizaciones de los sistemas operativos.	X		X		X		
7. Considera Ud., que se requieren de cuentas usuarios genéricos o por defecto para la operación de los sistemas	X		X		X		
8. Considera Ud., que es adecuado el sistema de inventarios de los equipos de red.	X		X		X		
9. Considera Ud., que los usuarios deben contar con un conocimiento adecuado sobre el Spoofing	X		X		X		
10. Considera Ud., en que se cuenta con una política de control de acceso documentada y revisada basada en los requisitos de negocio y seguridad de la información.	X		X		X		
11. Considera Ud., que debe contarse con una gestión de contraseñas que aseguran la calidad de las mismas.	X		X		X		
12. Considera Ud., que se realiza el cambio de contraseña cada cierto tiempo.	X		X		X		
<b>DISPONIBILIDAD</b>							
13. Considera Ud., que se realiza la verificación, revisión y evaluación de los controles de continuidad de seguridad de la información a intervalos regulares	X		X		X		
14. Considera Ud., en que las instalaciones de procesamiento de la información deben implementarse con	X		X		X		

redundancia suficiente para cumplir con requisitos de disponibilidad.	X		X		X		
15. Considera Ud., que debe estar implementado y documentado procesos, procedimiento y controles para asegurar la continuidad de seguridad de la información.	X		X		X		
16. Considera Ud., que se debe contar con metodologías de respaldo de información eficientes.	X		X		X		
17. Considera Ud., en que la protección de los equipos contra fallas de electricidad aseguran la disponibilidad de los sistemas de información.	X		X		X		
<b>INTEGRIDAD</b>							
18. Considera Ud., que debe realizarse periódicamente respaldos de información.	X		X		X		
19. Considera Ud., que la manipulación de datos debe ser realizado sin la alteración de los mismos.	X		X		X		
20. Considera Ud., que el antivirus instalado en su equipo debe encontrarse correctamente actualizado y lo proteja tanto de virus como de otras amenazas informáticas.	X		X		X		

**Observaciones (precisar si hay suficiencia):** Existe suficiencia para su aplicación

**Opinión de aplicabilidad:** Aplicable [ X ] Aplicable después de corregir [ ] No aplicable [ ]

**Apellidos y nombres del juez validador:** *M.s. Poletti Gaitán, Eduardo Humberto DNI. 18073124*

**Especialidad del validador:** *Docente investigador*

Lima, 20 de Abril del 2019

<sup>1</sup>**Pertinencia:** El ítem corresponde al concepto teórico formulado.

<sup>2</sup>**Relevancia:** El ítem es apropiado para representar al componente o dimensión específica del constructo

<sup>3</sup>**Claridad:** Se entiende sin dificultad alguna el enunciado del ítem, es conciso, exacto y directo

**Nota:** Suficiencia, se dice suficiencia cuando los ítems planteados son suficientes para medir la dimensión

  
Firma del Experto Informante

**CERTIFICADO DE VALIDEZ DE CONTENIDO DEL INSTRUMENTO QUE MIDE LA VARIABLE:  
DIGITALIZACIÓN DE DOCUMENTOS**

DIMENSIÓN	Pertinencia <sup>1</sup>		Relevancia <sup>2</sup>		Claridad <sup>3</sup>		Sugerencias
	Si	No	Si	No	Si	No	
<b>PROCESO</b>							
1. Considera Ud., en que la entidad posee un cuadro de clasificación de documentos.	X		X		X		
2. Considera Ud., que cuenta con ambientes adecuados para la conservación de documentos físicos recibidos para su preparación previa a su digitalización.	X		X		X		
3. Considera Ud., que son adecuados los formatos a utilizar para los diversos tipos de documentos.	X		X		X		
4. Considera Ud., que el documento digitalizado cuenta con la integridad y legibilidad suficiente	X		X		X		
5. Considera Ud., que siempre debe llevarse una Clasificación de los documentos originales de acuerdo con los problemas de digitalización que se presenten.	X		X		X		
6. Considera Ud., que es adecuado el tiempo requerido para la digitalización de documentos.	X		X		X		
7. Considera Ud., que los documentos digitalizados poseen cualidades de durabilidad, inalterabilidad y fijeza similares a los documentos originales	X		X		X		
8. Considera Ud., que los documentos digitalizados se encuentran accesibles.	X		X		X		
9. Considera Ud., en que el acceso a la información conservada en discos ópticos supone que permanecerá legible, inteligible y recuperable.	X		X		X		
10. Considera Ud., adecuado los controles empleados para archivar los documentos digitalizados.	X		X		X		
<b>NORMATIVA</b>							
11. Considera Ud., en que la intervención de un Fedatario Informático otorga valor legal al documento digitalizado.	X		X		X		
12. Considera Ud., en que se debe cumplir con la normativa que establece hacer una auditoría una vez al año.	X		X		X		
13. Considera Ud., que la organización debe contar con un programa de auditoría informática aplicable al sistema de digitalización.	X		X		X		
<b>SOPORTE TÉCNICO</b>							
14. Considera Ud., que se cuenta con los equipos de hardware adecuados para el trabajo de digitalización.	X		X		X		
15. Considera Ud., que los equipos de hardware (scáner) cuentan con los estándares de calibración para el trabajo de digitalización.	X		X		X		
16. Considera Ud., en que la arquitectura del sistema de digitalización mejora los componentes del sistema sin degradar sus funciones y sin perder información.	X		X		X		

17. Considera Ud., que el soporte de almacenamiento (Disco Externo NAS) se conserva en condiciones ambientales adecuadas.	X		X		X		
18. Considera Ud., que los softwares requeridos en la digitalización cuentan con licencia	X		X		X		
19. Considera Ud., en que el sistema puede acceder a la información ya digitalizada y convertirla a la nueva versión, permitiendo la transferencia de la información sin que sufra ninguna modificación.	X		X		X		
20. Considera Ud., que se tiene la documentación técnica relacionada con la Seguridad de la información en todos los componentes del sistema de digitalización debidamente conservada.	X		X		X		

**Observaciones (precisar si hay suficiencia):** Existe suficiencia para su aplicación

**Opinión de aplicabilidad:** Aplicable [X] Aplicable después de corregir [ ] No aplicable [ ]

**Apellidos y nombres del juez validador:** Dr. Lezama Gonzalez, Pedro DNI. 09656742

**Especialidad del validador:** Ing. de sistemas

Lima, 20 de Abril del 2019

<sup>1</sup>**Pertinencia:** El ítem corresponde al concepto teórico formulado.

<sup>2</sup>**Relevancia:** El ítem es apropiado para representar al componente o dimensión específica del constructo

<sup>3</sup>**Claridad:** Se entiende sin dificultad alguna el enunciado del ítem, es conciso, exacto y directo

**Nota:** Suficiencia, se dice suficiencia cuando los ítems planteados son suficientes para medir la dimensión

  
Firma del Experto Informante

**CERTIFICADO DE VALIDEZ DE CONTENIDO DEL INSTRUMENTO QUE MIDE LA VARIABLE:  
SEGURIDAD DE LA INFORMACIÓN**

DIMENSIÓN	Pertinencia <sup>1</sup>		Relevancia <sup>2</sup>		Claridad <sup>3</sup>		Sugerencias
	Si	No	Si	No	Si	No	
<b>CONFIDENCIALIDAD</b>							
1. Considera Ud., en que los usuarios cuentan con acceso a los servicios que han sido específicamente autorizados a usar.	X		X		X		
2. Considera Ud., en que el acceso a la información y a las funciones del sistema están restringidas en concordancia con la política de control de acceso.	X		X		X		
3. Considera Ud., que se tiene un adecuado inventario de accesos a los sistemas.	X		X		X		
4. Considera Ud., que los propietarios de los activos revisan los derechos de acceso de usuario en intervalos regulares.	X		X		X		
5. Considera Ud., que se cuenta con la configuración por defecto para el hardware y software de digitalización.	X		X		X		
6. Considera Ud., que se hacen efectiva las políticas de administración de configuraciones y actualizaciones de los sistemas operativos.	X		X		X		
7. Considera Ud., que se requieren de cuentas usuarios genéricos o por defecto para la operación de los sistemas.	X		X		X		
8. Considera Ud., que es adecuado el sistema de inventarios de los equipos de red.	X		X		X		
9. Considera Ud., que los usuarios deben contar con un conocimiento adecuado sobre el Spoofing.	X		X		X		
10. Considera Ud., en que se cuenta con una política de control de acceso documentada y revisada basada en los requisitos de negocio y seguridad de la información.	X		X		X		
11. Considera Ud., que debe contarse con una gestión de contraseñas que aseguran la calidad de las mismas.	X		X		X		
12. Considera Ud., que se realiza el cambio de contraseña cada cierto tiempo.	X		X		X		
<b>DISPONIBILIDAD</b>							
13. Considera Ud., que se realiza la verificación, revisión y evaluación de los controles de continuidad de seguridad de la información a intervalos regulares.	X		X		X		
14. Considera Ud., en que las instalaciones de procesamiento de la información deben implementarse con	X		X		X		

redundancia suficiente para cumplir con requisitos de disponibilidad.	X		X		X		
15. Considera Ud., que debe estar implementado y documentado procesos, procedimiento y controles para asegurar la continuidad de seguridad de la información.	X		X		X		
16. Considera Ud., que se debe contar con metodologías de respaldo de información eficientes.	X		X		X		
17. Considera Ud., en que la protección de los equipos contra fallas de electricidad aseguran la disponibilidad de los sistemas de información.	X		X		X		
<b>INTEGRIDAD</b>							
18. Considera Ud., que debe realizarse periódicamente respaldos de información.	X		X		X		
19. Considera Ud., que la manipulación de datos debe ser realizado sin la alteración de los mismos.	X		X		X		
20. Considera Ud., que el antivirus instalado en su equipo debe encontrarse correctamente actualizado y lo proteja tanto de virus como de otras amenazas informáticas.	X		X		X		

Observaciones (precisar si hay suficiencia): Existe suficiencia para su aplicación

Opinión de aplicabilidad: Aplicable [X] Aplicable después de corregir [ ] No aplicable [ ]

Apellidos y nombres del juez validador. *Dr. Lezama Gonzales, Pedro*  
DNI. 09656742

Especialidad del validador: *Ing. de sistemas*

Lima, 20 de Abril del 2019

<sup>1</sup>**Pertinencia:** El ítem corresponde al concepto teórico formulado.

<sup>2</sup>**Relevancia:** El ítem es apropiado para representar al componente o dimensión específica del constructo

<sup>3</sup>**Claridad:** Se entiende sin dificultad alguna el enunciado del ítem, es conciso, exacto y directo

**Nota:** Suficiencia, se dice suficiencia cuando los ítems planteados son suficientes para medir la dimensión

  
Firma del Experto Informante

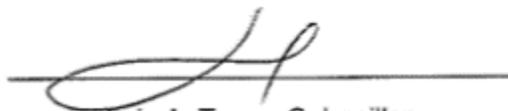
**Anexo No.07.**  
**Acta de originalidad**

### Acta de Aprobación de originalidad de Tesis

Yo, Luis A. Torres Cabanillas, docente de la Escuela de Posgrado de la Universidad César Vallejo filial Lima Norte, revisor de la tesis titulada "DIGITALIZACIÓN DE DOCUMENTOS Y SEGURIDAD DE LA INFORMACIÓN DE UN CENTRO SUPERIOR UNIVERSITARIO, LIMA NORTE, 2019." del estudiante **Marco Antonio Soto Martínez**, constato que la investigación tiene un índice de similitud de 15% verificable en el reporte de originalidad del programa Turnitin.

El suscrito analizó dicho reporte y concluyó que cada una de las coincidencias detectadas no constituye 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.

Lima, 14 de agosto del 2019



Luis A. Torres Cabanillas

DNI: 08404690

**Anexo No. 08**  
**Reporte turnitin**



**Anexo No. 09**  
**Formulario de autorización CRAI**



## FORMULARIO DE AUTORIZACIÓN PARA LA PUBLICATION ELECTRÓNICA DE LAS TESIS

### 1. DATOS PERSONALES

Apellidos y Nombres: (solo los datos del que autoriza)

SOTO MARTÍNEZ, MARCO ANTONIO

D.N.I. : 16682355

Domicilio : Psje. San Rodolfo 6793 - Los Olivos

Teléfono : Fijo : - Móvil : 965364184

E-mail : m.sotoma@ucv.edu.pe

### 2. IDENTIFICACIÓN DE LA TESIS

Modalidad:

Tesis de Pregrado

Facultad : .....

Escuela : .....

Carrera : .....

Título : .....

Tesis de Posgrado

Maestría

Doctorado

Grado : MAESTRO

Mención: INGENIERÍA DE SISTEMAS CON MENCIÓN EN TECNOLOGÍAS DE LA INFORMACIÓN

### 3. DATOS DE LA TESIS

Autor (es) Apellidos y Nombres:

SOTO MARTÍNEZ, MARCO ANTONIO

Título de la tesis:

DIGITALIZACIÓN DE DOCUMENTOS Y SEGURIDAD DE LA

INFORMACIÓN EN LA SECRETARÍA GENERAL DE UN

CENTRO SUPERIOR UNIVERSITARIO LIMA NORTE, 2019

Año de publicación : 2019

### 4. AUTORIZACIÓN DE PUBLICACIÓN DE LA TESIS EN VERSIÓN ELECTRÓNICA:

A través del presente documento, autorizo a la Biblioteca UCV-Lima Norte, a publicar en texto completo mi tesis.

Firma :

Fecha : 04/10/2019

**Anexo No. 10**  
**Autorización de la versión final**



# UNIVERSIDAD CÉSAR VALLEJO

## AUTORIZACIÓN DE LA VERSIÓN FINAL DEL TRABAJO DE INVESTIGACIÓN

CONSTE POR EL PRESENTE EL VISTO BUENO QUE OTORGA EL ENCARGADO DE INVESTIGACIÓN DE

### ESCUELA DE POSGRADO

A LA VERSIÓN FINAL DEL TRABAJO DE INVESTIGACIÓN QUE PRESENTA:

MARCO ANTONIO SOTO MARTÍNEZ

INFORME TÍTULADO:

DIGITALIZACIÓN DE DOCUMENTOS Y SEGURIDAD DE LA  
INFORMACIÓN EN LA SECRETARÍA GENERAL DE UN CENTRO  
SUPERIOR UNIVERSITARIO, LIMA NORTE, 2019

PARA OBTENER EL TÍTULO O GRADO DE:

MAESTRO EN INGENIERÍA DE SISTEMAS CON MENCIÓN EN TECNOLOGÍAS DE  
LA INFORMACIÓN

SUSTENTADO EN FECHA: 16 de Agosto de 2019

NOTA O MENCIÓN: APROBADO POR UNANIMIDAD



\_\_\_\_\_  
FIRMA DEL ENCARGADO DE INVESTIGACIÓN

**Anexo No.11**  
**Resultados descriptivos de las dimensiones**

## Resultados descriptivos de la Dimensión Proceso de Digitalización de Documentos

Tabla 16

Proceso de Digitalización de Documentos en la Secretaría General de un Centro Superior Universitario, Lima Norte 2019

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Poco eficiente	7	35,0	35,0	35,0
	Eficiente	13	65,0	65,0	100,0
	Total	20	100,0	100,0	

Fuente: Data de resultados obtenidos de la aplicación del cuestionario sobre Digitalización de Documentos.

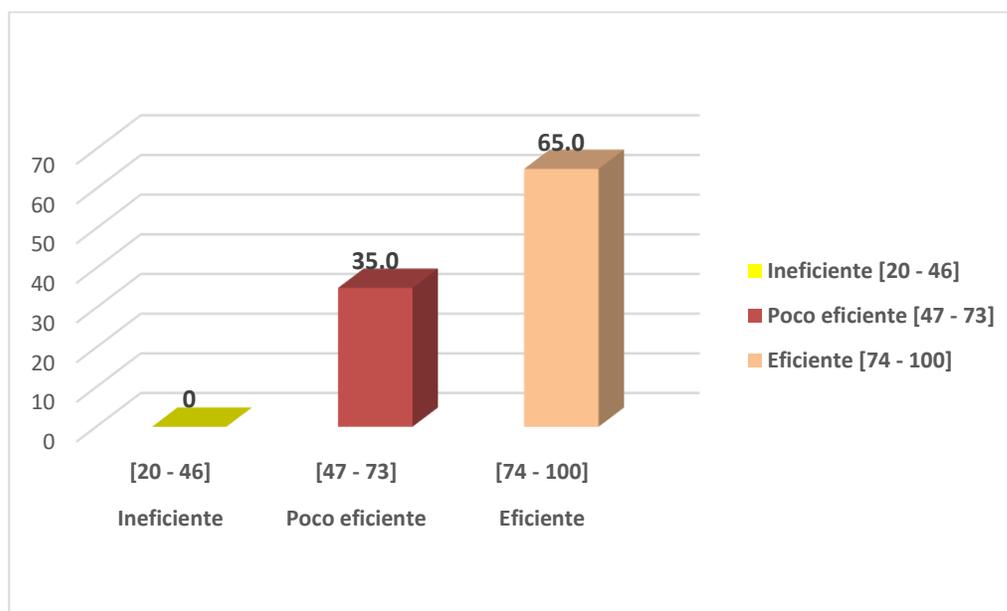


Figura 6. Proceso de Digitalización de Documentos en la Secretaría General de un Centro Superior Universitario, Lima Norte 2019.

### Interpretación:

De lo observado en la tabla 16 y figura 6; la base de datos no presenta para esta variable ningún valor perdido, de forma que las 20 observaciones son todas válidas. La tabla refleja que 7 trabajadores que equivalen el 35% de la muestra de estudio perciben que el Proceso de Digitalización de Documentos es Poco Eficiente; 13 trabajadores que equivalen al 65% de la

muestra de estudio percibe que el Proceso de Digitalización de Documentos es Eficiente. Esto significa que los trabajadores perciben que el Proceso de digitalización de documentos es Eficiente.

### Resultados descriptivos de la Dimensión Normativa de Digitalización de Documentos

Tabla 17

*Normativa de Digitalización de Documentos en la Secretaría General de un Centro Superior Universitario, Lima Norte 2019*

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Poco eficiente	5	25,0	25,0	25,0
	Eficiente	15	75,0	75,0	100,0
	Total	20	100,0	100,0	

Fuente: Data de resultados obtenidos de la aplicación del cuestionario sobre Digitalización de Documentos.

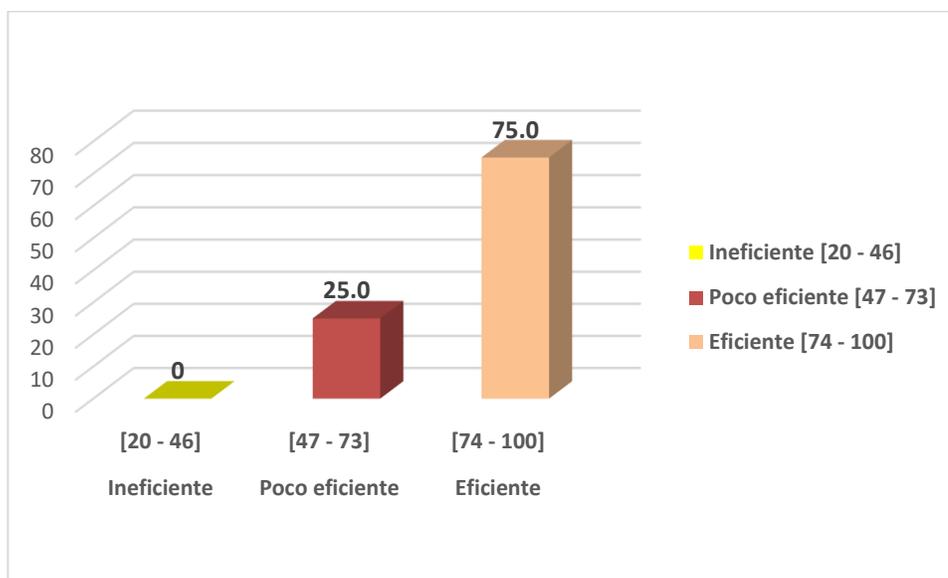


Figura 7. Normativa de Digitalización de Documentos en la Secretaría General de un Centro Superior Universitario, Lima Norte 2019.

### Interpretación:

De lo observado en la tabla 17 y figura 7; la base de datos no presenta para esta variable ningún valor perdido, de forma que las 20 observaciones son todas válidas. La tabla refleja que 5 trabajadores que equivalen el 25.0% de la muestra de estudio perciben que la Normativa de

Digitalización de Documentos es Poco Eficiente; 15 trabajadores que equivalen al 75.0% de la muestra de estudio percibe que la Normativa de Digitalización de Documentos es Eficiente. Esto significa que los trabajadores perciben que la Normativa de digitalización de documentos es Eficiente.

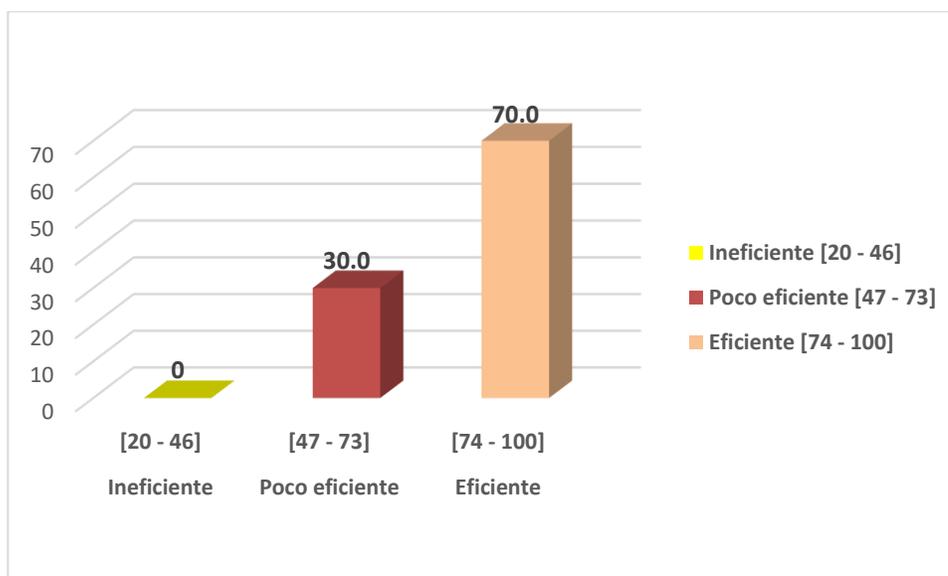
### Resultados descriptivos de la Dimensión Soporte técnico de Digitalización de Documentos

Tabla 18

*Soporte técnico de Digitalización de Documentos en la Secretaría General de un Centro Superior Universitario, Lima Norte 2019*

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Poco eficiente	6	30,0	30,0	30,0
	Eficiente	14	70,0	70,0	100,0
	Total	20	100,0	100,0	

Fuente: Data de resultados obtenidos de la aplicación del cuestionario sobre Digitalización de Documentos.



*Figura 8. Soporte técnico de Digitalización de Documentos en la Secretaría General de un Centro Superior Universitario, Lima Norte 2019.*

### Interpretación:

De lo observado en la tabla 18 y figura 8; la base de datos no presenta para esta variable ningún valor perdido, de forma que las 20 observaciones son todas válidas. La tabla refleja que 6 trabajadores que equivalen el 30.0% de la muestra de estudio perciben que el Soporte técnico de Digitalización de Documentos es Poco Eficiente; 14 trabajadores que equivalen al 70.0% de la muestra de estudio percibe que el Soporte técnico de Digitalización de Documentos es Eficiente. Esto significa que los trabajadores perciben que el Soporte técnico de digitalización de documentos es Eficiente.

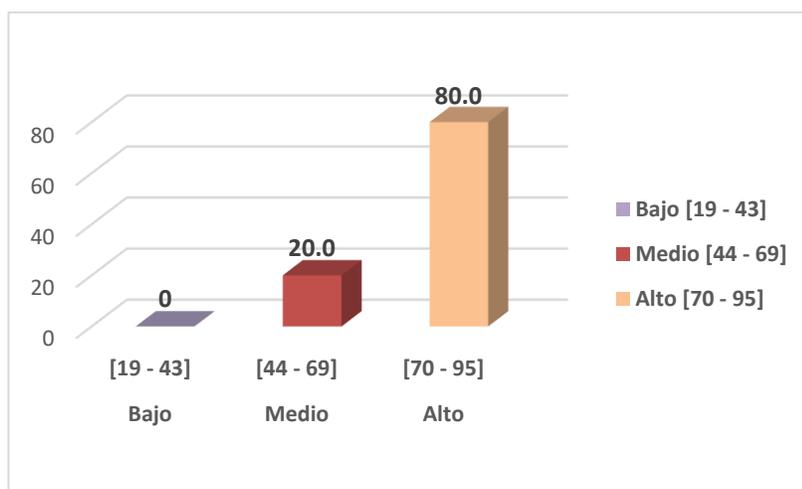
### Resultados descriptivos de la Dimensión Confidencialidad de la Información

Tabla 19

*Confidencialidad de la Información en la Secretaría General de un Centro Superior Universitario, Lima Norte 2019*

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Medio	4	20,0	20,0	20,0
	Alto	16	80,0	80,0	100,0
	Total	20	100,0	100,0	

Fuente: Data de resultados obtenidos de la aplicación del cuestionario sobre Seguridad de la Información.



*Figura 9. Confidencialidad de la Información en la Secretaría General de un Centro Superior Universitario, Lima Norte 2019.*

### Interpretación:

De lo observado en la tabla 19 y figura 9; la base de datos no presenta para esta variable ningún valor perdido, de forma que las 20 observaciones son todas válidas. La tabla refleja que 4 trabajadores que equivalen el 20.0% de la muestra de estudio perciben que la Confidencialidad de la Información es de nivel medio; 16 trabajadores que equivalen al 80.0% de la muestra de estudio percibe que la Confidencialidad de la Información es de nivel alto. Esto significa que los trabajadores perciben que la Confidencialidad de la Información es de nivel alto.

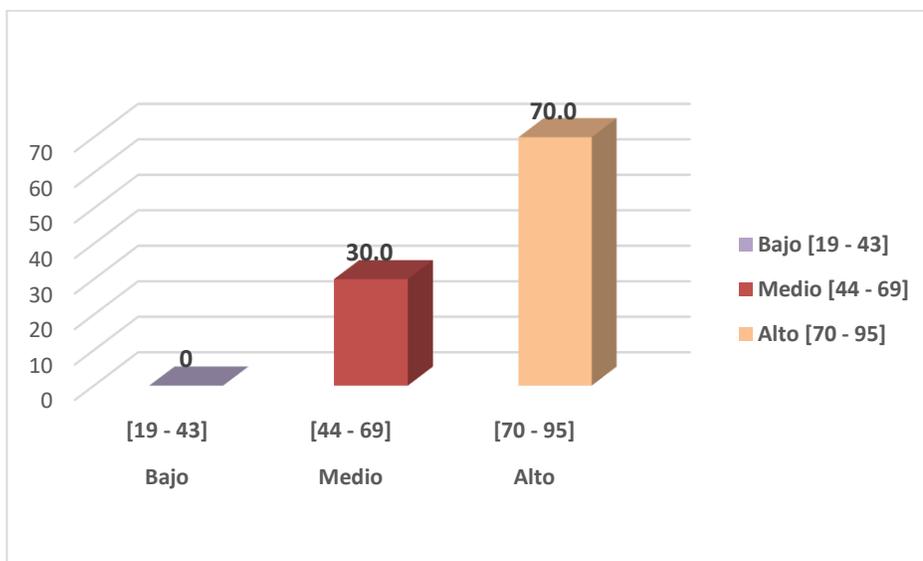
### Resultados descriptivos de la Dimensión Disponibilidad de la Información

Tabla 20

*Disponibilidad de la Información en la Secretaría General de un Centro Superior Universitario, Lima Norte 2019*

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Medio	6	30,0	30,0	30,0
	Alto	14	70,0	70,0	100,0
	Total	20	100,0	100,0	

Fuente: Data de resultados obtenidos de la aplicación del cuestionario sobre Seguridad de la Información.



*Figura 10.* Disponibilidad de la Información en la Secretaría General de un Centro Superior Universitario, Lima Norte 2019.

### Interpretación:

De lo observado en la tabla 20 y figura 10; La base de datos no presenta para esta variable ningún valor perdido, de forma que las 20 observaciones son todas válidas. La tabla refleja que 6 trabajadores que equivalen el 30.0% de la muestra de estudio perciben que la Disponibilidad de la Información es de nivel medio; 14 trabajadores que equivalen al 70.0% de la muestra de estudio percibe que la Disponibilidad de la Información es de nivel alto. Esto significa que los trabajadores perciben que la Disponibilidad de la Información es de nivel alto.

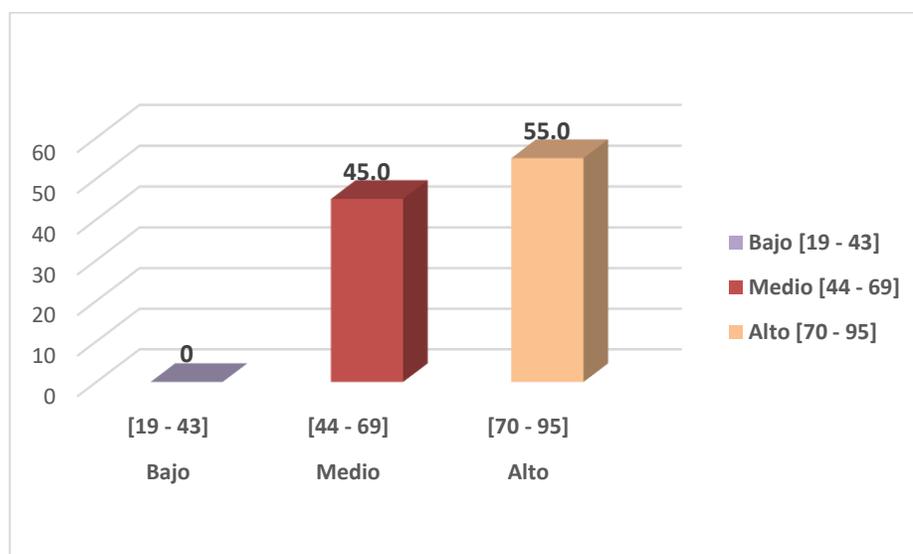
### Resultados descriptivos de la Dimensión Integridad de la Información

Tabla 21

*Integridad de la Información en la Secretaría General de un Centro Superior Universitario, Lima Norte 2019*

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Medio	9	45,0	45,0	45,0
	Alto	11	55,0	55,0	100,0
	Total	20	100,0	100,0	

Fuente: Data de resultados obtenidos de la aplicación del cuestionario sobre Seguridad de la Información.



*Figura 11. Integridad de la Información en la Secretaría General de un Centro Superior Universitario, Lima Norte 2019.*

### Interpretación:

De lo observado en la tabla 21 y figura 11; la base de datos no presenta para esta variable ningún valor perdido, de forma que las 20 observaciones son todas válidas. La tabla refleja que 9 trabajadores que equivalen el 45.0% de la muestra de estudio perciben que la Integridad de la Información es de nivel medio; 11 trabajadores que equivalen al 55.0% de la muestra de estudio percibe que la Integridad de la Información es de nivel alto. Esto significa que los trabajadores perciben que la Integridad de la Información es de nivel alto.

### Resultados descriptivos de las variables Digitalización de Documentos y Seguridad de la Información en la Secretaría General de un Centro Superior Universitario Lima Norte 2019.

Tabla 22

*Digitalización de Documentos \* Seguridad de la Información*

			Seguridad		Total
			Medio	Alto	
Digitalización de Documentos	Poco eficiente	Recuento	3	2	5
		% dentro de Digitalización de Documentos	15,0%	10,0%	25,0%
	Eficiente	Recuento	1	14	15
		% dentro de Digitalización de Documentos	5,0%	70,0%	75,0%
Total		Recuento	4	16	20
		% dentro de Digitalización de Documentos	20,0%	80,0%	100,0%
		% del total	100,0%	100,0%	100,0%

*Fuente: Cuestionario Digitalización de Documentos y Seguridad de la Información.*

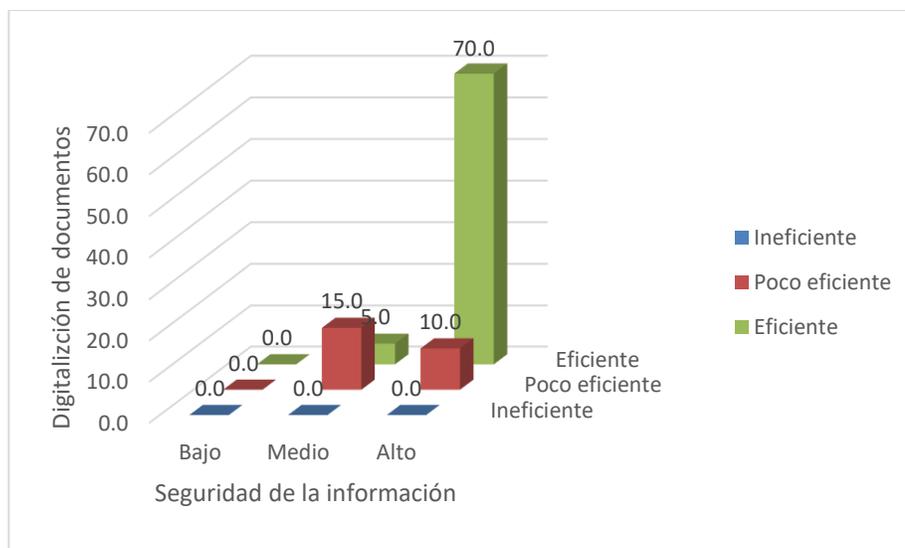


Figura 12. Digitalización de Documentos y Seguridad de la Información.

Se observa en la tabla 22 y la figura 12; el 15% del personal perciben que la Digitalización de Documentos está en el nivel poco eficiente y corresponde al nivel medio de Seguridad de la Información. El 70,0% del personal perciben que la Digitalización de Documentos está en el nivel eficiente y corresponde al nivel alto de Seguridad de la Información.

### Dimensión Proceso de Digitalización de Documentos y la variable Seguridad de la Información en la Secretaría General de un Centro Superior Universitario Lima Norte, 2019

Tabla 23

*Proceso de Digitalización de Documentos \* Seguridad de la Información*

Proceso de Digitalización de Documentos	Eficiencia	Recuento	Seguridad		Total
			Medio	Alto	
Proceso de Digitalización de Documentos	Poco eficiente	Recuento	3	2	5
		% dentro de Seguridad	15,0%	10,0%	25,0%
		% del total	15,0%	10,0%	25,0%
	Eficiente	Recuento	4	11	15
		% dentro de Seguridad	20,0%	55,0%	75,0%
		% del total	20,0%	55,0%	75,0%
Total	Recuento	7	13	20	
	% dentro de Seguridad	35,0%	65,0%	100,0%	
	% del total	100,0%	100,0%	100,0%	

Fuente: Cuestionario Digitalización de Documentos y Seguridad de la Información.

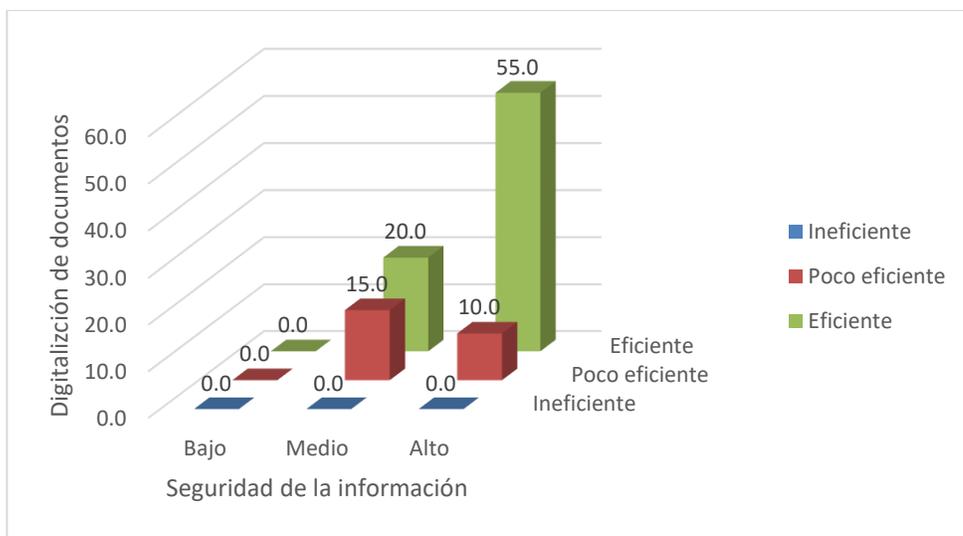


Figura 13. Proceso de Digitalización de Documentos y Seguridad de la Información.

Como se observa en la tabla 23 y la figura 13; el 15.0% del personal perciben que el Proceso de Digitalización de Documentos está en el nivel poco eficiente y corresponde al nivel medio de Seguridad de la Información. El 55.0% del personal perciben que el Proceso Digitalización de Documentos está en el nivel eficiente y corresponde al nivel alto de Seguridad de la Información.

### Dimensión Normativa de Digitalización de Documentos y la variable Seguridad de la Información en la Secretaría General de un Centro Superior Universitario Lima Norte, 2019.

Tabla 24

*Normativa de Digitalización de Documentos \* Seguridad de la Información*

			Seguridad		Total
			Medio	Alto	
Normativa de Digitalización de Documentos	Poco eficiente	Recuento	3	2	5
		% dentro de Seguridad	15,0%	10,0%	25,0%
		% del total	15,0%	10,0%	25,0%
	Eficiente	Recuento	3	12	15
		% dentro de Seguridad	15,0%	60,0%	75,0%
		% del total	15,0%	60,0%	75,0%
Total	Recuento	6	14	20	
	% dentro de Seguridad	30,0%	70,0%	100,0%	
	% del total	100,0%	100,0%	100,0%	

Fuente: Cuestionario Digitalización de Documentos y Seguridad de la Información.

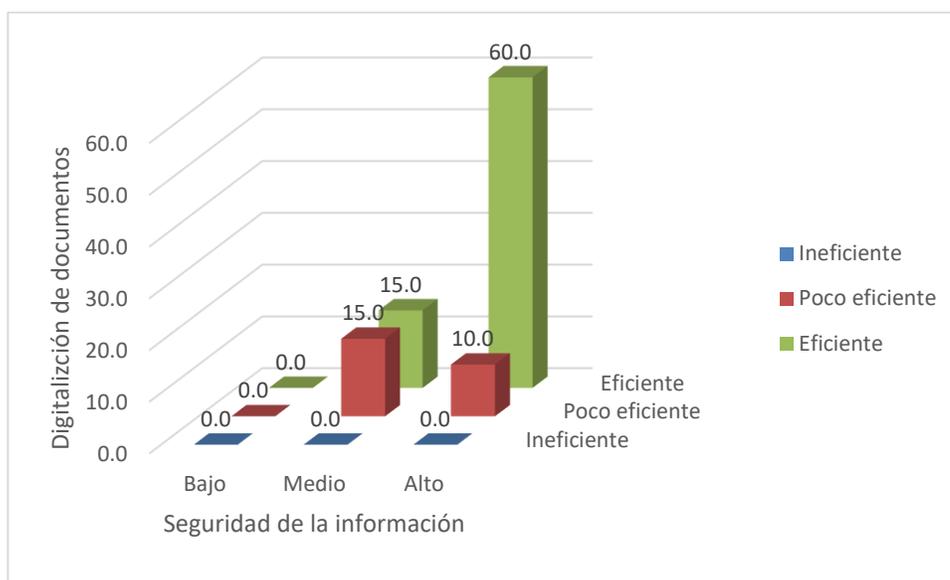


Figura 14. Normativa de Digitalización de Documentos y Seguridad de la Información.

Se observa en la tabla 24 y la figura 14; el 60% del personal perciben que la Normativa está en el nivel eficiente y corresponde al nivel alto de Seguridad de la Información. El 15 % del personal perciben que la Normativa de Digitalización de Documentos está en el nivel poco eficiente y corresponde al nivel medio de Seguridad de la Información. El 15% del personal perciben que la Normativa de Digitalización de Documentos está en el nivel eficiente y corresponde al nivel medio de Seguridad de la Información.

### Dimensión Soporte técnico de Digitalización de Documentos y la variable Seguridad de la Información en la Secretaría General de un Centro Superior Universitario Lima Norte 2019.

Tabla 25

Soporte técnico Digitalización de Documentos \* Seguridad de la Información

		Seguridad		Total	
		Medio	Alto		
Soporte técnico de Digitalización de Documentos	Poco eficiente	Recuento	3	5	8
		% dentro de Seguridad	15,0%	25,0%	40,0%
		% del total	15,0%	25,0%	40,0%
	Eficiente	Recuento	7	5	12
		% dentro de Seguridad	35,0%	25,0%	60,0%
		% del total	35,0%	25,0%	60,0%
Total	Recuento	10	10	20	
	% dentro de Seguridad	50,0%	50,0%	100,0%	
	% del total	100,0%	100,0%	100,0%	

Fuente: Cuestionario Digitalización de Documentos y Seguridad de la Información.

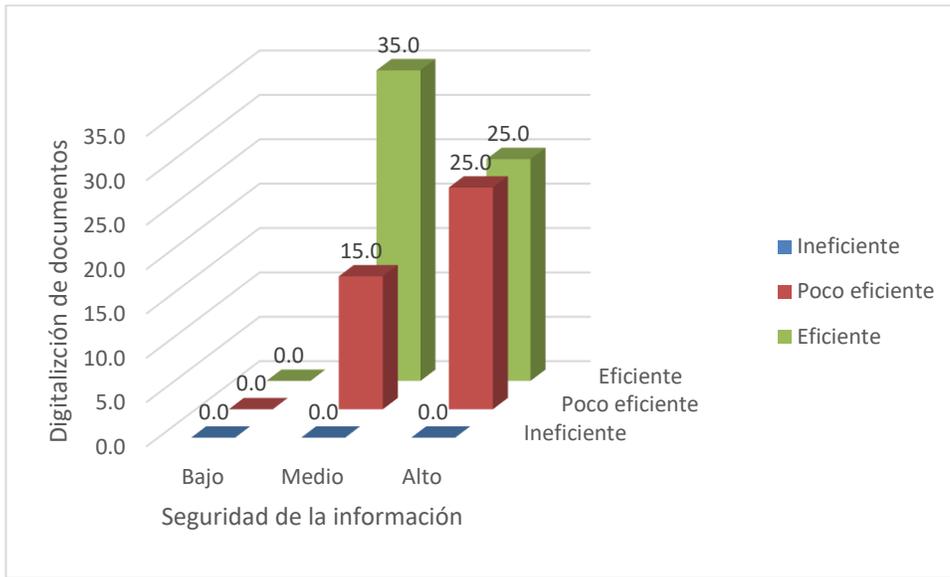


Figura 15. Soporte técnico Digitalización Documentos y Seguridad de la Información.

Como se observa en la tabla 25 y la figura 15; el 25% del personal perciben que el Soporte Técnico está en el nivel eficiente y corresponde al nivel alto de Seguridad de la Información. El 15% del personal perciben que el Soporte Técnico está en el nivel poco eficiente y corresponde al nivel medio de Seguridad de la Información. El 35% del personal perciben que el Soporte Técnico de Digitalización de Documentos está en el nivel eficiente y corresponde al nivel medio de Seguridad de la Información.