UNIVERSIDAD CÉSAR VALLEJO

ESCUELA DE POSGRADO

PROGRAMA ACADÉMICO DE MAESTRÍA EN INGENIERIA DE SISTEMAS CON MENCION EN TECNOLOGIAS DE INFORMACIÓN

DNI electrónico en la mejora del control de acceso a los sistemas de información en la Superintendencia Nacional de Educación Superior Universitaria, Lima 2021

TESIS PARA OBTENER EL GRADO ACADÉMICO DE:

Maestro en Ingeniería de Sistemas con Mención en Tecnologías de Información

AUTOR:

Arroyo Castro, Victor Alejandro (ORCID: 0000-0001-8870-179X)

ASESOR:

Dr. Visurraga Agüero, Joel Martin (0000-0002-0024-668X)

LÍNEA DE INVESTIGACIÓN:

Sistemas de información y Comunicaciones

LIMA – PERÚ

2021

Dedicatoria

A Dios por ser forjador de mi camino, a mis padres por cada bendición a lo largo de mi vida y a mi pareja por su amor, por animarme a creer en mí.

Agradecimiento

Agradezco a mi pareja por su asesoría, apoyo y aliento durante el desarrollo de esta tesis y por sus constantes consejos para lograr la realización de esta tesis.

Índice de contenidos

Índice de tablas

Índice de gráficos figuras

Resumen

La presente investigación tiene como objetivo general determinar que el DNI electrónico mejora en el control de acceso a los sistemas de información en la Superintendencia Nacional de Educación Superior Universitaria, Lima 2021. Mediante esta investigación se mide las variables DNI electrónico y control de acceso a los Sistemas de información con indicadores Índice de accesos no autorizados, Índice de tiempo de respuesta e Índice de disponibilidad de servicio.

El tipo de investigación empleada es aplicada y el diseño de la investigación es experimental puro. Asimismo, se tiene la población de 50 observaciones para medir los tres indicadores ante un pre-test y post-test respectivamente obtenidas mediante un muestreo probabilístico. La técnica de recolección de datos es la observación y como instrumento de recolección de datos es la guía de observación.

Los resultados permitieron llegar a la conclusión que el DNI electrónico mejora significativamente el control de acceso a los sistemas de información como se demuestra en el estado de los indicadores índice de accesos no autorizados donde se redujo a un 91,16%, del mismo modo mejoró el índice de tiempo de respuesta a un 81,16%, además el índice de disponibilidad de servicio aumento a un 78,99%.

Palabras clave: DNI electrónico, control de acceso y sistemas de información.

Abstract

The general objective of this research is to determine that the electronic DNI improves in the control of access to information systems in the National Superintendency of Higher University Education, Lima 2021. Through this research the variables electronic DNI and access control to the Information systems with indicators Unauthorized access index, response time index and service availability index.

The type of research used is applied and the research design is pure experimental. Likewise, there is a population of 50 observations to measure the three indicators before a pre-test and post-test, respectively, obtained through probability sampling. The data collection technique is observation and as a data collection instrument it is the observation guide.

The results allowed us to conclude that the electronic DNI significantly improves the control of access to information systems as shown in the status of the indicators Unauthorized access index where it was reduced to 91.16%, in the same way it improved the Response Time Index to 81.16%, and the Service Availability Index increased to 78.99%.

Keywords: Electronic DNI, Access Control and Information Systems.

I. INTRODUCCIÓN

En la actualidad a nivel mundial se ha acelerado el avance tecnológico y por consiguiente se observa que el número de usuarios se ha un incrementado en la forma que acceden a los sistemas de información de manera tradicional; sin embargo, el avance tecnológico ha hecho que la mayor parte sean vulnerables, esto ha dado lugar a un aumento posterior en el número de casos de delitos informáticos.

En el intercambio electrónico de datos, es aún más difícil abordar los problemas básicos de seguridad relacionados con el control de acceso. Mientras suma el número de usuarios y servicios en línea, también lo hace la cantidad de casos de robo y fraude de datos personales, las estrategias de seguridad tradicionales como contraseñas simples y muros inapropiados hace fuente débil de autorización y casi al instante hace frágil la inseguridad informática.

Actualmente con tecnologías informáticas más poderosas y efectivas, dispositivos de almacenamiento móviles y biometría, es posible implementar un control de acceso más eficaz para ayudar a reducir los casos de seguridad de la información.

En el Perú a nivel normativo los lineamientos de seguridad los define la SEGDI, la cual no indica información sobre el control de acceso, además no hay un entendimiento claro sobre la responsabilidad general de la seguridad de la información en los sistemas informáticos, cabe añadir que los responsables notorios son los departamentos de Tecnologías.

En la Superintendencia Nacional de Educación Superior Universitaria el control de acceso que se tiene a los diferentes aplicativos informáticos se lleva a cabo a través de un sistema denominado Punku (Puerta), que funge de puerta de entrada a los diferentes sistemas de información.

El mayor problema se tiene en el control de acceso a la información de la Superintendencia Nacional de Educación Superior Universitaria que tiene un núcleo de diseño débil, esto se debe a que se basa en tecnología implementada hace más

de 4 años. Muchos sistemas de información están experimentando actualmente algunos ataques y problemas operativos graves porque ofrecen menos protección durante la autenticación. Esto ha llevado a una mayor alza de robo y fraude de datos personales que se encuentran en la mayoría de los servicios en línea en la actualidad. Por lo tanto, existe una necesidad urgente de un sistema de acceso de control digital en tiempo real que logre satisfacer las necesidades de los usuarios de los sistemas informáticos.

La presente investigación responde a la pregunta formulada como problema general ¿De qué manera el DNI electrónico mejora en el Control de acceso a los sistemas de información en la Superintendencia Nacional de Educación Superior Universitaria, Lima 2021?

Así mismo, como problemas específicos: (a) ¿De qué manera el DNI electrónico mejora el índice accesos no autorizados en el Control de acceso a los sistemas de información en la Superintendencia Nacional de Educación Superior Universitaria, Lima 2021?, (b) ¿De qué manera el DNI electrónico mejora el índice de tiempo de respuesta en el Control de acceso a los sistemas de información en la Superintendencia Nacional de Educación Superior Universitaria, Lima 2021? y (c) ¿De qué manera el DNI electrónico mejora el índice de disponibilidad de servicio en el Control de acceso a los sistemas de información en la Superintendencia Nacional de Educación Superior Universitaria, Lima 2021?

En cuanto a las justificaciones se indican a continuación: En la justificación epistemológica es fundamental considerar sobre cómo la investigación contribuye al tema de ciertas variables en el campo de la institución de estudio. Las contribuciones se pueden combinar con otras originales e innovadoras, no solo construyendo nuevos enfoques a temas ya buscados en este campo, sino también brindando diferentes perspectivas sobre temas que se exploran desde diferentes áreas del conocimiento.

La justificación teórica de la presente investigación amplia el conocimiento moderno con respecto a DNI electrónico, especialmente a la mejora del Control de acceso a los sistemas de información en la Superintendencia Nacional de

Educación Superior Universitaria de Lima en el año 2021, información proporcionada como base para las actividades de implementaciones futuras de proyectos electrónicos.

La justificación práctica de la presente investigación da a conocer que existen principales beneficios que se obtendrían al implementar nuevas tecnologías, esto favorecerá a las instituciones públicas y privadas inicien proyectos para brindar servicios de control de acceso utilizando DNI electrónico, así también como una oportunidad de actualización en beneficio de los usuarios.

Por último, la justificación metodológica de la presente investigación permitirá conocer el control de acceso a la Superintendencia Nacional de Educación Superior Universitaria realizando los métodos propuestos y así elaborar y realizar una propuesta de mejora, así mismo dar beneficio a los colaboradores en el manejo de su información otorgándoles herramientas que permitan la seguridad en el control de acceso.

Con relación, al objetivo general se busca, determinar que el DNI electrónico mejora en el Control de acceso a los sistemas de información en la Superintendencia Nacional de Educación Superior Universitaria, Lima 2021.

A continuación se detallan los objetivos específicos: (a) Determinar que el DNI electrónico mejora el índice accesos no autorizados en el control de acceso a los sistemas de información en la Superintendencia Nacional de Educación Superior Universitaria, Lima 2021, (b) Determinar que el DNI electrónico mejora el índice de tiempo de respuesta en el Control de acceso a los sistemas de información en la Superintendencia Nacional de Educación Superior Universitaria, Lima 2021 y (c) Determinar que el DNI electrónico mejora el índice de disponibilidad de servicio en el control de acceso a los sistemas de información en la Superintendencia Nacional de Educación Superior Universitaria, Lima 2021

De igual manera se planteó la hipótesis general: El DNI electrónico mejora significativamente en el Control de acceso a los sistemas de información en la Superintendencia Nacional de Educación Superior Universitaria, Lima 2021.

Con respecto a las hipótesis específicas, se mencionan a continuación: (a) El DNI electrónico mejora significativamente el índice accesos no autorizados en el Control de acceso a los sistemas de información en la Superintendencia Nacional de Educación Superior Universitaria, Lima 2021, (b) El DNI electrónico mejora significativamente el índice de tiempo de respuesta en el Control de acceso a los sistemas de información en la Superintendencia Nacional de Educación Superior Universitaria, Lima 2021 y (c) El DNI electrónico mejora significativamente el índice de disponibilidad de servicio en el Control de acceso a los sistemas de información en la Superintendencia Nacional de Educación Superior Universitaria, Lima 2021.

II. MARCO TEÓRICO.

Para sustentar el presente trabajo se identificaron estudios previos; respecto a los antecedentes nacionales a Yañez (2019) en su investigación cuyo objetivo es identificar el dominio de un sistema de identificación facial para el control de acceso; en su respectiva investigación determina que, dado el tiempo promedio de espera antes y después del programa fue 2,40 minutos, concluyendo la espera en el laboratorio de computación de las diferentes facultades se redujo significativamente con la ayuda del sistema de identificación facial y control de acceso. Asimismo, el programa introducido se ha reducido a 1,52 minutos por alumno. Por lo tanto, la aplicación redujo la demora de acceso a promedio en 0.88 minutos por estudiante, dado que el acceso previo a la implementación del sistema alcanzo el 97%de precisión, donde el número de acceso al laboratorio de las diversas facultades de diversas carreras aumento rápidamente el apoyo del sistema de control de acceso con reconocimiento facial. Y una vez implementado el proceso de selección, se logró el 100% de éxito de los estudiantes. Por ello, se puede enfatizar que la aplicación de sistemas de control de acceso se cree que ha reducido el acceso no autorizado en un 3%, también se observa que la tasa de asistencia al laboratorio de cómputo está subiendo rápidamente con la ayuda del sistema, ya que el número de participantes antes de la apertura del sistema fue del 67%. Asimismo, la asistencia de los estudiantes, una vez realizado el proceso de selección, asistió el 80% de los estudiantes. Por tanto, se concluye que la aplicación de sistemas antes mencionado ha incrementado el valor de los participantes, así como también incrementó en la participación de los universitarios en un 23%, esto se debe a los controles de acceso que el sistema de identificación facial mejoró en la atención de los alumnos en el laboratorio.

Por otra parte, Espinoza (2018) con su investigación cuyo objetivo es el desarrollo para la implementación de seguridad inalámbrica en el control de acceso para los usuarios; menciona sobre su ardua investigación sobre el desarrollo a un sistema de control de acceso centrado en tecnología inalámbrica la cual abre

oportunidades limitadas. Al mismo tiempo la comunicación que plantea se realiza mediante diferentes dispositivos, esto permite el acceso a la red. Por lo tanto, autenticación de contraseña evalúa el acceso telefónico, a través del trabajo diferente de protección de datos, esto incluye el uso de medidas de seguridad, uso de protocolo. El control de acceso además los protocolos de autenticación se utilizan en medidas de seguridad, significa la ruta que se verifica de varias maneras. Los parámetros utilizados en el proceso de control de acceso de validación y autorización son lo que permiten el acceso desde la red local y un mayor control sobre los usuarios. Por lo cual proporciona un sistema para determinar el nivel de origen del usuario. Así también utiliza un protocolo en la aplicación inalámbrica. La conclusión de su investigación demuestra que los sistemas de seguridad de control de acceso que utilizaron, controlan el nivel de autenticación y autorización para controlar el tráfico inalámbrico.

En cuanto a Martínez (2018) con su investigación cuyo objetivo es implementar un sistema de control de acceso a red; demuestra los resultados del análisis e interpretación sobre el control de acceso a red, que considera necesario la implementación que cumpla con las expectativas de las empresas privadas debido al alto nivel de satisfacción con los usuarios, dando a notarse que esta lectura corresponde al presente estudio, describiendo implementar un sistema de control de acceso a red en diferentes empresas privadas de las provincias. Por ello se ha llegado a la conclusión del estudio realizando una evaluación técnica que pudo confirmar los requisitos mínimos de equipamiento y en software para un diseño estándar y sistema de control de acceso de usuarios para dichas empresas que se mencionó anteriormente, evaluando los eventos que se ejecutaron en libretas de direcciones, como servidores Linux y Windows. Esto ayudo a establecer los valores mínimos proporcionados por el sistema, el entorno de desarrollo se evalúa de forma más apropiada y ayuda a proporcionar el máximo beneficio del sistema propuesto, donde fundamentalmente es la implementación del sistema de gestión dando mejoría a la seguridad de las cuentas de diversos usuarios de la red.

Asimismo, Martínez (2018) en su investigación cuyo objetivo es analizar la implementación del DNI electrónico, en su investigación resalta las bondades de esta esta implementación y del documento nacional de identidad electrónico que permite una autenticación segura y confiable de la identidad de los usuarios que transfieren información digital electrónicamente. Así, cada usuario es responsable del flujo de información civil, penal, administrativa o funcional y atribuye al proceso el respectivo peso de autoridad y propiedad irrevocables, su estudio concluye permitiendo autenticar la identidad de los usuarios en los medios de internet, así mismo ofrece el tratamiento digital de la información.

Finalmente, respecto a los antecedentes nacionales se tiene a Neira (2017) con su investigación cuyo objetivo principal es el uso de la visión artificial que identificará el documento de identidad de una persona; en su trabajo de investigación presenta su triunfo demostrando que es posible implementar un sistema de control de acceso que identifica al número del certificado de un país mediante una pantalla temporal. Esto es importante para capturar la luz y la distancia desde la cámara al punto de vista. Si se utiliza un haz de infrarrojos claro y no se ajusta a la distancia, la identificación puede ser diferente debido al tamaño de identificación diferente en el momento de la recolección, (por ejemplo, un algoritmo, funcional debido a las diferentes medidas). El DNI azul se ve forzado por un filtro suave después de la captura, esto se puede separar con éxito migrando del modelo RGB al modelo HSV. Esto facilita la separación del DNI de la pared de imágenes y la alta resolución de las imágenes del DNI tanto como la distancia de recuperación a la que constituyen a que sea muy exitoso para comprender los números utilizados de la biblioteca de detección de Huellas dactilares, A dependiendo de la resolución, las cámaras web de alto rendimiento dan excelentes resultados, concluye con el éxito de su implementación y reconocimiento de DNI utilizando la visión artificial y recalca la importancia de la iluminación y distancia para la detección.

En cuanto a los antecedentes internacionales, se analizó a Cao et al (2021) en su investigación cuyo objetivo es diseñar un mecanismo de control de acceso

basado en tokens con mecanismo inteligentes con ajuste dinámico de las reglas de control de acceso, que garantiza que solo los usuarios autorizados pueden activar y ejecutar contratos inteligentes específicos. Luego propone un mecanismo de detección para detectar ataques en contra de forma efectiva y real; con base en estos mecanismos también propone un marco de control de acceso y detección de intrusos para resistir varios ataques manteniendo todas las características y funcionalidades del subyacente basado en blockchain finaliza realizando una evaluación integral que demuestra que es seguro factible y eficiente. Por otro lado, Yua et al (2021) centran su investigación en el análisis de los requisitos de control de acceso empresarial en el despacho de la red eléctrica y sistema de control, estudia tecnologías clave relacionadas a través del sistema de prototipos de verificación, logra que estas tecnologías resuelven los problemas de control de acceso en la nueva arquitectura del sistema.

Asimismo, Ummer y Ajaz (2020) con su investigación cuyo objetivo fue lograr la autenticación entre un nuevo nodo y pueda convertirse en parte de la red, posteriormente, después de la debida autenticación de un nuevo nodo, establece una clave compartida con todos. En su conclusión proponen un mecanismo de control de acceso seguro y escalable para el entorno de IoT. El esquema propone un mecanismo para el despliegue de nuevos dispositivos inteligentes dentro de la capa de percepción de las aplicaciones de IoT. Por consiguiente, Gupta y Megha (2018) con su investigación titulada, Un marco de control de acceso basado en identidad y autenticación mutua para servicios de computación en la nube distribuidos en entornos IoT mediante tarjetas inteligentes, cuyo objetivo fue proponer un marco que implica el uso de tarjetas inteligentes por parte de los usuarios para acceder a los servicios y datos basados en la nube en un entorno de IoT distribuido, además de un marco de autenticación de tarjeta inteligente basado en criptografía de curva elíptica en el que se utiliza una sola tarjeta inteligente utilizado para acceder a múltiples aplicaciones. En la conclusión final enfocan su investigación en el entorno de IoT de computación en la nube distribuida con dispositivos de IoT con recursos limitados y proponen un marco novedoso para

proporcionar a los usuarios acceso a diferentes servicios en la nube utilizando la misma contraseña credenciales y tarjeta inteligente.

Por consiguiente, Yue et al (2020) con su investigación cuyo objetivo fue proporcionar un enfoque seguro, escalable y ligero, diseñaron un esquema de control de acceso de IoT apoyado en capacidades utilizando la descentralización basada en blockchain identificador realizado como una solución. Se concluye presentando un enfoque de control de acceso de IoT basado en capacidades en el diseño de la arquitectura, aprovechan la cadena de bloques y la descentralización del identificador para permitir a los usuarios administrar sus diferentes identidades relaciones y credenciales para la concesión de derechos de acceso. Por otra parte, Shantanu et al (2020) con su investigación titulada Control de acceso a Internet de las cosas: tecnologías asistencia habilitada: una arquitectura, desafíos y requisitos; cuyo objetivo fue proporcionar una básica introducción a la tecnología de asistencia, proporcionar descripciones del IoT y discutir el surgimiento de tecnología de asistencia habilitada para IoT. Se concluye detallando la necesidad de control de acceso seguro dentro de los sistemas de asistencia habilitados para IoT, examinaron un conjunto de requisitos para los dispositivos de asistencia habilitados para IoT, además discuten un enfoque para acceder a los sistemas mediante seguridad de control de acceso.

Además, Rubio y Gómez (2017) menciona en su trabajo de investigación realizado en España-Madrid, que una identificación digital proporciona un certificado electrónico que identifique al usuario, cuyo objetivo es aprovechar el uso de los certificados digitales que contiene el DNI electrónico. Sin embargo, no se usa mucho en la comunidad, no es una herramienta que facilite el uso de estos certificados por parte de los gobiernos, sino que se enfoca en desarrollar aplicaciones para uso interno sin monitorear las aplicaciones diarias y las condiciones de los activos domésticos. Es por ello sería recomendable la solución de dicho problema, siendo más fácil para el usuario y que requiera menos esfuerzo para usarla desde una perspectiva o diferente. Asimismo, el desarrollo de este proyecto con certificados o documentos de identidad electrónica es un gran desafío y un gran esfuerzo por

lograr, puesto que no hay documentos emitidos por el gobierno que de la facilidad a la navegación de internet y los dispositivos que acceden a internet, estos están experimentando muchos cambios en la actualidad. Además, las aplicaciones que implementan servicios de autenticación utilizando documentación digital original consideran todas las solicitudes para facilitar el uso por parte de desarrolladores o personas. Por otro lado, dado algunos dispositivos de escritorio se utilizan como ID para crear firmas digitales siendo esta función más utilizada para desarrollar uno de los métodos más usables en el internet para diferente software y muchos otros. Concluye indicando la importancia DNI para la autenticación del usuario y la firma de documentos digitales con igual validez.

Finalmente, respecto a los antecedentes internacionales se tiene a Ragesh y Baskaran (2016) con su investigación cuyo objetivo fue analizar la seguridad de su esquema propuesto y su evaluación de desempeño en los sistemas de registros médicos personales. Se concluye proponiendo un esquema de cifrado basado en conjuntos de atributos para abordar el problema de revocación de atributos en múltiples sistemas de registros médicos personales asistidos por la nube.

La siguiente investigación toma como base la siguiente teoría: Teoría general de sistemas. De acuerdo con Loor et al (2019) los autores argumentaron respecto a la Teoría general de sistema desde su perspectiva que un sistema es un todo organizado conformado de componentes que interrelaciona de una forma determinada y esta posición sistémica posee varias aplicaciones en diferentes ramas de la ciencia como son la biología, las matemáticas, la química, la física, la educación, la sociología o la psicología etc. Además. Rezende y Abreu (2010) confirma el origen de la teoría general de sistemas y la importancia en la investigación y desarrollo relacionados con el sistema en general, sus esfuerzos se centran en generar conceptos capaces de generar condiciones aplicables en realidades empíricas y prácticas de las cuestiones científicas del sistema.

Por otra parte, Hans (1994) indica que la Teoría general de sistemas puede transformarse fácilmente en un conjunto de procedimientos y además pueden concebirse en un software ajustable. Por otro lado, Weilkiens (2007) sostiene que

la teoría general de sistemas está en un nivel muy abstracto; transfiriéndolo a un campo concreto de conocimiento, podemos derivar muchas herramientas, métodos importantes y específicos. El pensamiento sistemático nos permite interactuar con los sistemas sin conocer los detalles de los componentes individuales de los que están compuestos.

Asimismo, Sieniutycz (2020) afirma que la Teoría general de sistemas es una ciencia que investiga las leyes generales para arreglos arbitrariamente complejos que constituyen integridades funcionales y está vinculada con la teoría de la información. Finalmente, Cummings (2001) indica que una premisa clave de la teoría general de sistemas tiene que ver con la definición de un sistema y cómo forma un todo organizado, este se compone de partes y relaciones entre ellos, proporciona el marco u principio de organización para estructurar las partes y las relaciones en un todo organizado.

Por otro lado, la teoría que respalda la investigación es la teoría de evolución tecnológica, de acuerdo con Torres et al (2019) los autores mencionan sobre La evolución tecnológica que son instrumentos prácticos, efectivos y de utilidad en el plano educativo, ya que nos facilita manejar de grandes volumenes de información que permiten ser procesados de manera veloz y servida a muchas personas y zonas impensables. La inversión en tecnología facilita que en cuanto a educación llegue a zonas y comunidades impensados. Por otra parte, Bessant y Pavitt (2005) explica que tiene sus raíces en las ideas existentes y se caracteriza por un cambio gradual, incluye pequeños cambios en la tecnología ya utilizada o aplicada y mejorada en nuevas situaciones.

Por otra parte, Coccia (2019) sostiene que la evolución tecnológica consiste en sustituir una nueva tecnología por la anterior, como la sustitución de carbón por madera, hidrocarburos por carbón, tecnología robótica para humanos, etc. Estos avances tecnológicos están representados por sustituciones competitivas de un método de satisfacer una necesidad de otro. Asimismo, para Bardeen y Cerpa. (2015) refieren que la teoría de evolución tecnológico des globa directo en las adaptaciones como los individuos pueden adaptarse a condiciones variantes en su

entorno, siendo los ecosistemas adaptables a nuevas especies, de la misma forma la evolución de la tecnología es una conversión de mejora.

Igualmente, Bixter et al (2018) mencionan que la teoría de la evolución tecnológica es la compenetración exacta del hoy que facilita la participación social, familiar, etc. Realizando acceso a las interacciones directas en tiempo real permitiendo conectarse de un mismo lugar a diferentes espacios mediante diferentes aparatos tecnológicos avanzados. Finalmente. Teece (2010) afirma que la tecnología evoluciona construyendo nuevos dispositivos y métodos a partir de los que existían anteriormente y a su vez ofreciéndolos como posibles combinaciones para la construcción de nuevos dispositivos y elementos. Las tecnologías de alguna manera deben surgir como nuevas combinaciones de lo que ya existe. Esta combinación de componentes y ensamblajes para nuevos productos y procesos se organiza en sistemas para algún propósito humano y tiene un orden jerárquico y recursivo.

En cuanto a la definición de la variable independiente DNI electrónico, se ha considerado lo siguiente. De acuerdo a PAE (2016) refiere sobre paeal DNI electrónico como identidad electrónica de un individuo, es el documento válido de efecto legal, también de poder firmar de manera digital documentos electrónicos, dándosele una validez jurídica semejante a la firma manuscrita. Así también el DNI electrónico tiene un chip, que conlleva datos iguales que muestran impresos en la tarjeta (fotografía, datos personales, huella dactilar digitalizada y firma digitalizada) integrado con la firma electrónica. Por lo tanto, las personas realizaran diferentes gestiones por internet de manera más segura con las entidades Públicas y privadas, en cualquier momento y sin realizar largas colas.

Por otro lado, Yrivarren (2015) indica sobre La identidad digital en certificados digitales facilita en acreditar que una persona determinada es quien dice ser en internet, de forma inequívoca, de igual modo Valles et al (2020) los autores comentan en relación al DNI electrónico que varias entidades públicas y privadas vienen implementando la firma digital de documentos desde años posteriores. también profesionales independientes se han integrado a esta modalidad de firma

digital. Se necesita contar primero con certificado digital. En la actualidad se realiza a través del certificado digital la cual viene en el DNI electrónico, este documento tiene una vigencia de dos años. El DNI electrónico se renueva en la Reniec.

Asimismo, Chao et al (2011) define la identificación digital electrónico de utilización segura, también conocido como acreditación digital, evolucionado rápidamente en los últimos años siendo hoy en día reemplazo de sus contrapartes basadas en papel o laminas. Además, se están capitalizando cada vez más los datos que permiten el reconocimiento exacto de identificación de la persona siendo así de mayor confiablidad. Por otro lado, Chin-Ling et al (2008) sostiene, a la identidad electrónica digital, como la capacidad de interoperar. Además, como el mejor aliado de accesibilidad, es decir en cualquier lugar donde uno se encuentre.

En cuanto la variable dependiente control de acceso a los sistemas de información, Laudon y Laudon (2016) indican que la infraestructura tecnológica es la se encarga de proporcionar la plataforma ahí es donde la entidad puede armar los sistemas de información que necesita. Cada entidad debe implantar con mucha destreza posible su infraestructura tecnológica, ya que será administrada previa capacitación de los colaborados, de esta manera brindará los servicios tecnológicos que la entidad necesita para la realización de sus funciones en el proceso de negocio con los sistemas de información.

Por otro lado, Lapiedra et al (2015) dichos autores comentaron al control acceso como un sistema de información con relación a las tablas interconectadas, la cual se soporta sobre un base de datos normalizada en función a lo que se necesite, que la entidad lo considere precisa para el desarrollo de las actividades necesarias. Además, indican a este como un componente determinado en recopilar, manejar, limpiar y procesar la información.

En cuanto a Aqsa y Colomo (2018) Manifiestan que el control de acceso es un mecanismo de autenticación sólida que emplea un seguro de datos que utiliza el software. A si también, la disponibilidad de servicios de solo usuarios autorizados que contenga su contraseña para el uso seguro de Internet, páginas web, almacenamiento seguro de datos en medios externos e internos. Además, Filippos

et al (2018) presentan un Sistema de Control de acceso automatizado como un servicio para controlar la actividad de los usuarios, para transmitir cualquier información de forma segura, proporciona una variedad de servicios con el objetivo de informar al administrador de la infraestructura las actividades de los usuarios o solicitudes de acceso que requieren permiso en función de suscripciones o criterios de autorización capaces de tratar de forma segura la información confidencial al tiempo que garantiza la seguridad e intimidad de los usuarios. Finalmente, Olakanmi y Dunun (2020) mencionan en su investigación que el control de acceso se adopta en un enfoque de seguridad de dos capas como la clave simétrica y el cifrado que se puede modificar basado en atributos para proporcionar control de acceso detallado en revocación eficiente e integridad de los datos, adoptando niveles de seguridad y protección para el proveedor. Además, el cifrado es uno de los enfoques utilizados para hacer cumplir el control de acceso, la integridad y la privacidad con exactitud.

La variable control de acceso a los sistemas de información va a ser medida por los siguientes indicadores (a) Índice de accesos no autorizados, (b) Índice de tiempo de respuesta y (c) Índice de disponibilidad de servicio. Se empieza a detallar a cada uno a continuación.

El Índice de accesos no autorizados, de acuerdo a Acurio. (2016) indica el acceso no autorizado a un sistema informático, se refiere en acceder de manera no permitida, contra derecho o sin autorización sobre un sistema de información, con la finalidad de lograr una satisfacción de carácter intelectual por el descubrimiento de las claves de acceso o password.

De acuerdo a Gómez (2020) comenta sobre acceso no autorizado en su estudio, y precisa como “una cierta prevención que evite la realización de intervenciones no autorizadas a una red o sistema informática, ya que estos efectos producen alteraciones en la información, garantizar su confidencialidad, integridad o autenticidad, reducir el funcionamiento de los equipos informáticos o incomunicar el acceso al sistema de usuarios autorizados”

De igual modo, Arellano y Ochoa (2015) indica que el acceso no autorizado se tiene que evaluar a través de la vulneración de medidas de seguridad; no se trata, por consiguiente, de conductas malintencionadas. Conservarse en el sistema o parte de este en oposición de la voluntad de quien posea el legítimo derecho de descartarlo.

Finalmente, Romero y Figueroa (2018) definen acceso no autorizado como Intrusismo Informático y se refiere como el comportamiento consistente en la introducción en sistemas de información o computadoras incumpliendo medidas de seguridad orientadas a proteger los datos contenidos en ella.

Por otra parte, el Índice de tiempo de respuesta, de acuerdo a Sepulveda y de Jesus (2018) se refiere el tiempo que demora ese proceso en una organización o entidad pública o privada que tiene la actividad de servicio al usuario, que tiene como objetivo brinda una respuesta efectiva y precisa para conseguir que los clientes sientan que se están atiendo sus consultas y servicios.

Además, Romero (2015) el autor comenta sobre tiempo de respuesta, definiendo la complejidad de factores que se involucran en la calidad del servicio y que brinda una organización o entidad ya sea pública o privada. Ya que sirve de base para medir el crecimiento y desarrollo de la entidad, por medio de la eficiencia y eficacia del tiempo que esta ofrece a sus usuarios.

Asimismo, Chydzins y Adamczyk (2020) define al tiempo de respuesta como el total de tiempo que un paquete aceptado pasa en el sistema, incluido el tiempo de servicio de este paquete. Tradicionalmente, los paquetes descartados son no contado en absoluto.

Finalmente, RajSudhakar et al (2021) refieren al tiempo de respuesta que es el tiempo transcurrido entre la activación y la finalización de un trabajo de una tarea, una tarea puede experimentar interferencia de mayor prioridad, retrasando así la finalización de un trabajo.

Por último, el Índice de disponibilidad de servicio, de acuerdo a Sepulveda y de Jesus (2018) la disponibilidad de servicios consiste en la capacidad de cierto

componente de configuración o de un servicio TI la cual cumple sus funciones establecidas al momento que lo soliciten. estas acciones son definidas por la mantenibilidad, confiabilidad, seguridad, rendimiento y capacidad de servicio.

Asimismo, Rogel (2018) el autor denomina disponibilidad a la posibilidad de un servicio o un bien que está presente en el momento que este se lo necesite. De eso se trata disponibilidad es la posibilidad de resolver problemas, dar resultados, o simplemente suministrar una ayuda limitada.

Finalmente, Cevallos (2018) comenta sobre la disponibilidad de servicio que es un factor importante respecto a servicios se refieren ya sea de una entidad privada o pública, la cual es el tiempo que dispone para solucionar y atender un servicio o un bien; así mismo, Covarrubias (2015) define sobre la Disponibilidad que consiste en el nivel en que un sistema o equipo está en condiciones operables para ser llamado en un momento donde lo requieran.

III. METODOLOGÍA

3.1. Tipo y diseño de investigación

Tipo de investigación

La presente investigación es de tipo aplicada, según Hernández, Fernández y Baptista (2014) manifiestan que la exploración es de condición aplicada dado que construye, modifica y se aplica en un contexto que es concreta, en la aplicación busca una solución rápida y práctica sobre el problema que se está tratando ya aplicada anteriormente, este tipo de investigación pretende dar solución a un problema que afecta a lo anteriormente investigado en conocido por el investigador.

Diseño de investigación

El diseño utilizado en la investigación es experimental del tipo puro, según Hernández et al (2014) expresan al diseño experimental como la recopilación de datos en el cual se compara las medidas del comportamiento en un grupo de control con respecto al grupo experimental como mínimo, el investigador controla deliberadamente los datos aleatoriamente.

Esquema:

RG: O_1 → X → O_2

Pre-test → DNI electrónico→ Post-Test

R=Asignación al azar

G=Grupo Experimental

X=Tratamiento

O_1-O_2=mediciones pre-test/ post-test del control de acceso a los sistemas de información

3.2. Variables y Operacionalización

Variable independiente: DNI electrónico

La variable independiente DNI electrónico es de tipo cuantitativa discreta. Este tipo de variable cuantitativa tiene la propiedad de que los datos se pueden recuperar mediante un procedimiento de conteo o registro.

Definición conceptual de la variable independiente - DNI electrónico

PAE (2016) refiere al DNI electrónico como identidad electrónica de un individuo, es el documento válido de efecto legal, también de poder firmar de manera digital documentos electrónicos, dándosele una validez jurídica semejante a la firma manuscrita. Así también el DNI electrónico tiene un chip, que conlleva datos iguales que muestran impresos en la tarjeta (fotografía, datos personales, huella dactilar digitalizada y firma digitalizada) integrado con la firma electrónica. Por lo tanto, las personas realizaran diferentes gestiones por internet de manera más segura con las entidades Públicas y privadas, en cualquier momento y sin realizar largas colas.

Variable dependiente: Control de acceso a los sistemas de información

La variable dependiente proceso de control de acceso a los sistemas de información es de tipo cuantitativa. Este tipo de variable cuantitativa tiene la propiedad de que los datos se pueden recuperar mediante un procedimiento de conteo o registro.

Definición conceptual de la variable - Control de acceso a los sistemas de información

Aqsa y Colomo (2018) manifiestan que el control de acceso es un mecanismo de autenticación sólida que emplea un seguro de datos que utiliza el software. A si también, la disponibilidad de servicios de solo usuarios autorizados que contenga su contraseña para el uso seguro de Internet, páginas web, almacenamiento seguro de datos en medios externos e internos.

Definición operacional de la variable - Control de acceso a los sistemas de información

En la siguiente tabla se muestra los tres indicadores que son el (a) Índice de accesos no autorizados, (b) Índice de tiempo de respuesta y el (c) Índice de disponibilidad de servicio. Donde se puede visualizar la formula respectiva de cada uno de los indicadores, así como la unidad de medida en la tabla 1.

Tabla 1

Matriz de operacionalización de la variable dependiente control de acceso a los sistemas de información

Indicadores	Instrumento	U. M	Fórmula
Índice de accesos no autorizados	Guía de Observación	**%**	$X = \frac{Nº\ de\ accesos\ no\ autorizados}{Nº\ total\ de\ accesos}\ x\ 100$
Índice de tiempo de respuesta	Guía de Observación	%	$X = \frac{Nº\ de\ tiempo\ de\ respuesta\ en\ los\ acceso}{Nº\ de\ tiempo\ total\ de\ accesos}\ x\ 100$
Índice de disponibilidad de servicio	Guía de Observación	%	$X = \frac{Nº\ de\ accesos\ atendidos}{Nº\ total\ de\ accesos\ solicitados}\ x\ 100$

Nota: Se visualiza la operacionalización de la variable dependiente.

La matriz de control de acceso a los sistemas de información se muestra en el Anexo 02.

3.3. Población, muestra y muestreo

Población

En el presente trabajo investigación se describe a la población en el cual se consideró de acuerdo a la cantidad a observar, esto se cuantificará en 50 observaciones para medir los tres indicadores ante un pre-test y post-test respectivamente.

Según Hernández et al (2014) mencionan a la población como el conjunto total de elementos, entidades donde sus características son similares o también conocido como universo o individuos dónde se utilizan cómo unidades de muestreo, así mismo es llamado como el universo de estudio donde se representa por la letra N en la fórmula correspondiente.

Tabla 2

Población de la investigación

Población	Cantidad	Indicador
Observaciones	50	Índice de accesos no autorizados
Observaciones	50	Índice de tiempo de respuesta
Observaciones	50	Índice de disponibilidad de servicio

Nota: Cuadro de población.

Muestreo

El tipo de muestreo seleccionado es probabilístico, según Hernández et al (2014) mencionan que en el muestreo probabilístico su designación se da mediante elementos que requiere de la probabilidad, selecciona una pequeña porción de la muestra a indagar; además, toda la población tiene igual probabilidad de ser escogido para la muestra, donde se obtiene estableciendo las propiedades o características de la población y el tamaño de muestra. La técnica usada fue muestreo aleatorio simple a excepción de reemplazo.

3.4. Técnicas e instrumentos de recolección de datos

Técnicas de recolección de datos

La presente investigación empleará en la recolección de datos la técnica de la observación, según Hernández et al (2014) definen a esta técnica de forma múltiple de obtener información, del cual depende la validez del estudio. Conjuntamente, indica que la técnica observación consiste en recolectar información ordenada,

valida y confiable del comportamiento y procesos observables mediante los indicadores.

Instrumentos de recolección de datos

Para la presente investigación se empleó la guía de observación. Para Hernández et al (2014) mencionan que los instrumentos de medida de acuerdo a la recolección de datos son recursos que permiten obtener los datos cuantitativos o recolectar información.

Tabla 3

Ficha técnica del instrumento

Nombre del instrumento:	Guía de observaciones de medición del indicador
Autor:	Victor Alejandro Arroyo Castro
Año:	2021
Descripción:	
Tipo de Instrumento:	Guía de observación
Objetivo:	Determinar que el DNI electrónico mejora en el control de acceso a los sistemas de información en la Superintendencia Nacional de Educación Superior Universitaria, Lima 2021.
Indicadores:	a) Índice de accesos no autorizados b) Índice de tiempo de respuesta c) Índice de disponibilidad de servicio
Número de observaciones a recolectar:	50
Aplicación:	Directa

Nota: Datos del instrumento.

Validez

En el presente trabajo se utilizó la validación en juicio de expertos, estos serán compuestos por tres profesionales expertos en la materia. Según Hernández et al (2014) definen la validez como el valor en que un instrumento cuantifica la variable que intenta demostrar. La validez de la presente investigación se determinó a través de juicio de expertos combinado por tres profesionales conectados con la temática; de acuerdo con Valderrama (2013) menciona que el juicio de expertos está combinado por un grupo de personas, en el que cada uno de ellos emiten un dictamen del instrumento, valorando la claridad, pertinencia y relevancia; este, con sentido lógico y empleando toda su expertiz.

Tabla 4

Expertos que validaron el instrumento de recolección de datos cuantitativos

DNI	Grado académico, apellido y nombres	Institución donde labora	Calificación
46830084	Mg. Ramirez Jaramillo Humbert Jasmin	SUNEDU	Aplicable
10095653	Dra. Vera Nuñez Griselda Gladys	Universidad Cesar Vallejo	Aplicable
10192315	Dr. Visurraga Agüero Joel Martín	Universidad Cesar Vallejo	Aplicable

Nota: Información de la validación de expertos.

3.5. Procedimientos

El procedimiento que se utilizó en la presente investigación, siguió las siguientes etapas: como primera etapa se elaboró el instrumento de recolección de datos utilizando la guía de observación, en la segunda etapa se determinó la validez de los instrumentos por parte de juicios de expertos, finalmente se realizó la descripción de las comparaciones correspondientes (pretest y postest) de los tres indicadores.

3.6. Método de análisis de datos

Para el análisis de los datos registrados de la actual investigación se realizó en lo que requiere al pre-test y post-test, se utilizó las herramientas digitales como Microsoft Excel y el aplicativo IBM SPSS v22. En cuanto al análisis descriptivo, se utilizará figuras y tablas, exponiendo medidas de tendencia central usando la media, se procederá su lectura o interpretación por indicador y datos emitidos por el instrumento, lo cual permitirá disponer una visual y estructurado entendimiento sencillo del total de datos numéricos. Finalmente, para el análisis inferencial, se comprobó la normalidad de los datos obtenidos mediante la prueba Test de Shapiro Wilk debido a que los datos son 50 observaciones; además, para la contrastación de la hipótesis se utilizó la prueba no paramétrica t de Wilcoxon.

3.7. Aspectos éticos

Para garantizar la integridad de la presente investigación se cumplió los principios de acuerdo a los reglamentos y lineamientos de la Universidad César Vallejo - Resolución de consejo 0262-2020UCV, las cuales sustentan la correcta transparencia y veracidad de la información. Cabe destacar la confiabilidad de la investigación que fue normada según APA. Aceptando la autenticidad de todo lo indicado y expresado, se asumió el compromiso y la responsabilidad de las políticas del uso ético y jurídico, manteniendo y respetando la privacidad de lo señalado. Además, para la autenticidad de los datos y para respetar las políticas anti plagio, se hizo uso del software Turnitin.

IV. Resultados

Análisis descriptivos

Medidas descriptivas del indicador: Índice de accesos no autorizados

Tabla 5

Medidas descriptivas del indicador: Índice de accesos no autorizados

	N	Mínimo	Máximo	Media	Desviación estándar
Indicador 1 – Pre-Test	50	55,65	88,89	80,6912	7,10376
Indicador 1 – Post-Tes	50	0,49	21,30	7,1320	5,36543
N válido (por lista)	50				

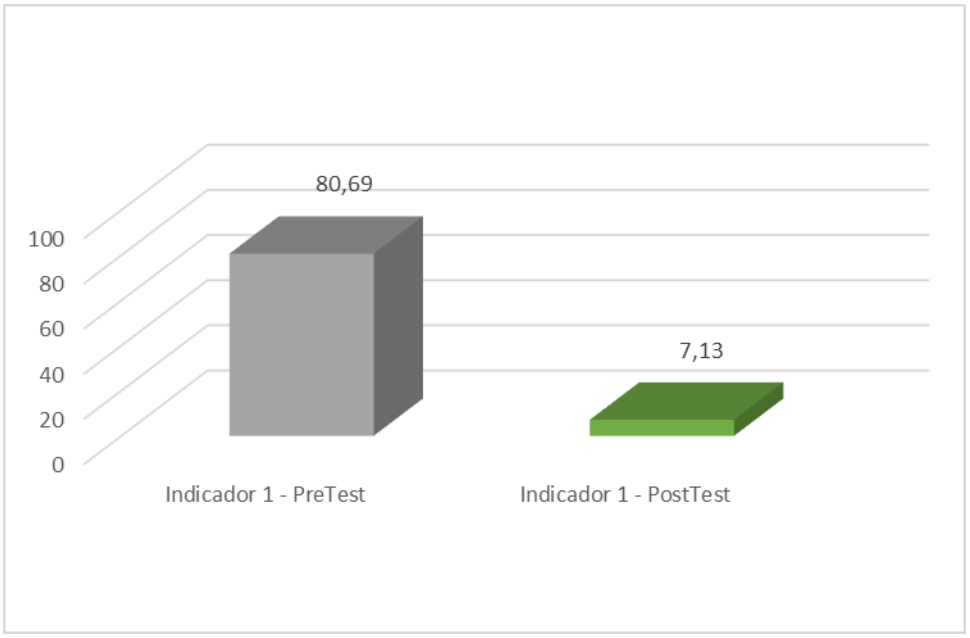
Nota: Datos asistido en el Software IBM SPSS v22.

En la tabla 5 se muestra los datos descriptivos del indicador índice de accesos no autorizados, en el pre-test de la muestra se observa que la media es 80,6912 veces y el valor del post-test es de 7,1320 veces que se redujo. En resumen, existe una mejora importante luego de implementar el DNI electrónico. Del mismo modo, es preciso señalar que la media en ambos casos se encuentra más cerca de los rangos mínimos en tanto que la desviación estándar promedio en el pre-test es 7,10376 y el post-test es 5,36543 donde se desvían de la media.

Asimismo, en el anexo 8(a) tenemos el gráfico de línea que nos permite visualizar la fluctuación de las tomas del pre-test y post-test del índice de accesos no autorizados.

Figura 1

Índice de accesos no autorizados antes y después de la aplicación con el DNI electrónico



Nota: Elaborado con asistencia del software Microsoft Excel.

En la figura 1 se refleja el antes y después de la implementación del DNI electrónico el cual muestra el comportamiento del indicador índice de accesos no autorizados en base a los datos obtenidos en la guía de observación, por lo tanto, se concluye que el índice de tiempo de respuesta la mejora se dio en la disminución en un 91,16% ó 73.56 veces.

Medidas descriptivas del indicador: Índice de tiempo de respuesta

Tabla 6

Medidas descriptivas del indicador: Índice de tiempo de respuesta

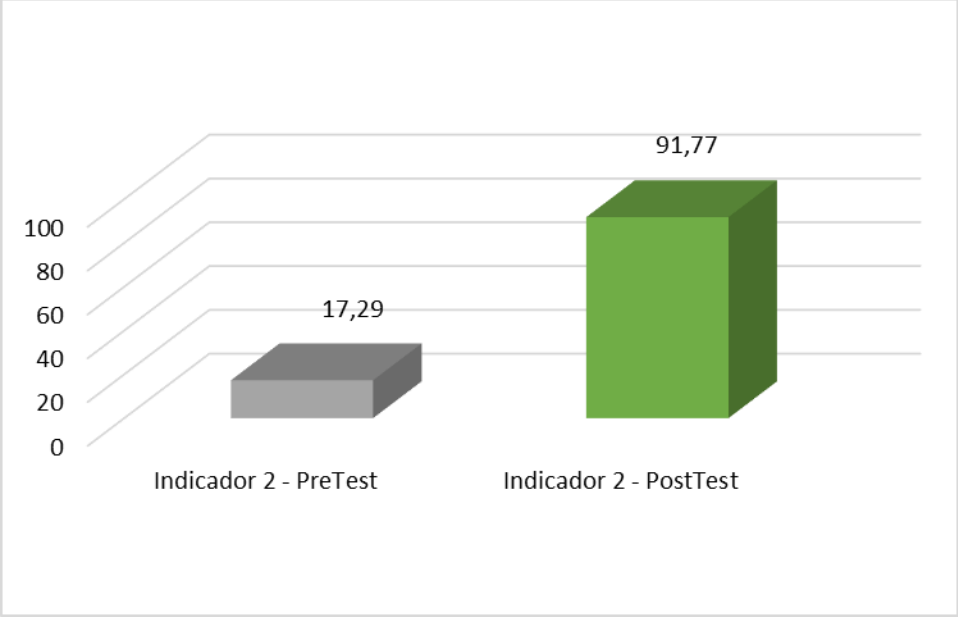
	N	Mínimo	Máximo	Media	Desviación estándar
Indicador 2 – Pre-Test	50	7,00	39,63	17,2944	8,25949
Indicador 2 – Post-Test	50	81,70	99,82	91,7712	5,72889
N válido (por lista)	50				

Nota: Datos asistido en el Software IBM SPSS v22.

En la tabla 6 se muestra los datos descriptivos del indicador índice de tiempo de respuesta, en el pre-test de la muestra se observa que la media es 17,2944 veces y el valor del post-test es de 91,7712 veces que aumento los rendimientos. En resumen, existe una mejora importante luego de implementar el DNI electrónico. Del mismo modo, es preciso señalar que la media en ambos casos se encuentra más cerca a los rangos mínimos en tanto que la desviación estándar promedio en el pre-test es 8,25949 y para el post-test es 5,72889 donde se desvían de la media. Asimismo, en el anexo 8(b) tenemos el gráfico de línea que nos permite visualizar la fluctuación de las tomas del pre-test y pos-test del índice de tiempo de respuesta.

Figura 2

Índice de tiempo de respuesta antes y después de la aplicación con el DNI electrónico



Nota: Elaborado con asistencia del software Microsoft Excel.

En la figura 2 se refleja el antes y después de la implementación del DNI electrónico el cual muestra el comportamiento del indicador índice de tiempo de respuesta en base a los datos obtenidos en la guía de observación, por lo tanto, se concluye que

el índice de tiempo de respuesta la mejora se dio en el aumento en un 81,16% ó 74.48 veces.

Medidas descriptivas del indicador: Índice de disponibilidad de servicio

Tabla 7

Medidas descriptivas del indicador: Índice de disponibilidad de servicio

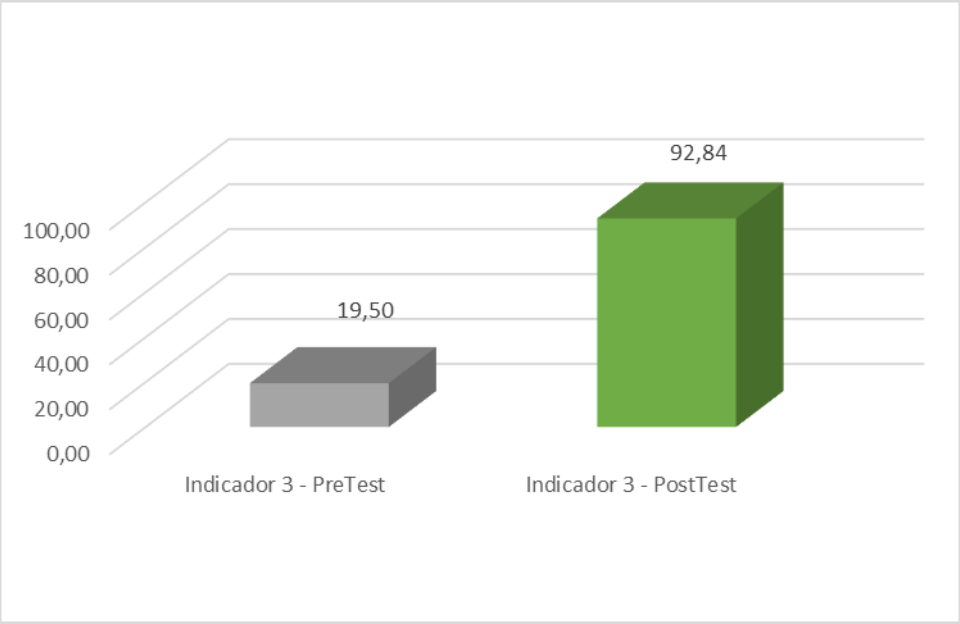
	N	Mínimo	Máximo	Media	Desviación estándar
Indicador 3 – Pre-Test	50	10,78	44,49	19,4994	7,80349
Indicador 3 – Post-Test	50	82,88	100,00	92,8356	5,66782
N válido (por lista)	50				

Nota: Datos asistido en el Software IBM SPSS v22.

En la tabla 7 se muestra los datos descriptivos del indicador índice de disponibilidad de servicio, en el pre-test de la muestra se observa que la media es 19,4994 veces y el valor del post-test es de 92,8356 veces que se aumentó rendimientos. En resumen, existe una mejora importante luego de implementar el DNI electrónico. Del mismo modo, es preciso señalar que la media en ambos casos se encuentra más cerca a los rangos mínimos en tanto que la desviación estándar promedio en el pre-test es 7,80349 y para el post-test es 5,66782 donde se desvían de la media. Asimismo, en el anexo 8(c) tenemos el gráfico de línea que nos permite visualizar la fluctuación de las tomas del pre-test y post-test del índice de disponibilidad de servicio.

Figura 3

Índice de disponibilidad de servicio antes y después de la aplicación con el DNI electrónico



Nota: Elaborado con asistencia del software Microsoft Excel.

En la figura 3 se refleja el antes y después de la implementación del DNI electrónico el cual muestra el comportamiento del indicador índice de disponibilidad de servicio en base a los datos obtenidos en la guía de observación, por lo tanto, se concluye que el índice de tiempo de respuesta la mejora se dio en el aumento en un 78,99% ó 73.34 veces.

Análisis Inferencial

Prueba de hipótesis

Para la presente investigación se ha realizado la prueba de hipótesis para cada uno de los indicadores; según Galindo (2020), señala que para los datos que siguen en la prueba de normalidad una distribución normal se empleará la prueba de t Student para pruebas relacionadas y para los datos que tienen una distribución no normal se utilizará las pruebas de Wilcoxon para pruebas relacionadas. Para esta

investigación se empleó la prueba de Wilcoxon para los 3 indicadores ya que siguen una distribución no normal.

Hipótesis específica 1: Índice de accesos no autorizados

Formulación de la hipótesis estadística:

H_0: El DNI electrónico no mejora significativamente el índice de accesos no autorizados en el control de acceso a los sistemas de información en la Superintendencia Nacional de Educación Superior Universitaria, Lima 2021.

H_1: El DNI electrónico mejora significativamente el índice de accesos no autorizados en el control de acceso a los sistemas de información en la Superintendencia Nacional de Educación Superior Universitaria, Lima 2021.

Considerando que el resultado de la prueba de normalidad del índice de accesos no autorizados no es normal (ver anexo 7), se aplicó la prueba de Wilcoxon.

Tabla 8

Prueba de Wilcoxon del indicador: Índice de accesos no autorizados

	Prueba de rangos con signo de Wilcoxon	
	Z	Sig. Asint. (bilateral)
Índice de accesos no autorizados Pre-test – Post-test	-6,154	,000

Nota: Datos asistido en el Software IBM SPSS v22.

Contrastación de hipótesis:

Para la contrastación de la hipótesis se realizó la prueba de Wilcoxon, se visualiza en la tabla 8 que el valor de significancia es de 0.000 hallándose menor al valor alfa de 0.05 por lo que se rechaza la hipótesis nula (H_0) y se acepta la hipótesis alterna (H_1). De igual forma, el valor de Z es de -6.154, se ubica en la zona de rechazo de la hipótesis nula; por lo tanto, el DNI electrónico mejora significativamente el índice de accesos no autorizados en el control de acceso a los sistemas de información en la Superintendencia Nacional de Educación Superior Universitaria, Lima 2021.

Hipótesis específica 2: Índice de tiempo de respuesta

Formulación de la hipótesis estadística:

H_0: El DNI electrónico no mejora significativamente el índice de tiempo de respuesta en el control de acceso a los sistemas de información en la Superintendencia Nacional de Educación Superior Universitaria, Lima 2021.

H_1: El DNI electrónico mejora significativamente el índice de tiempo de respuesta en el control de acceso a los sistemas de información en la Superintendencia Nacional de Educación Superior Universitaria, Lima 2021.

Considerando que el resultado de la prueba de normalidad del índice de tiempo de respuesta no es normal (ver anexo 7), se aplicó la prueba de Wilcoxon.

Tabla 9

Pruebas de Wilcoxon del indicador: Índice de tiempo de respuesta

	Prueba de rangos con signo de Wilcoxon	
	Z	Sig. Asint. (bilateral)
Índice de tiempo de respuesta Pre-test – Post-test	-6,154	,000

Nota: Datos asistido en el Software IBM SPSS v22.

Contrastación de hipótesis:

Para la contrastación de la hipótesis se realizó la prueba de Wilcoxon, se visualiza en la tabla 9 que el valor de significancia es de 0.000 hallándose menor al valor alfa de 0.05 por lo que se rechaza la hipótesis nula (H_0) y se acepta la hipótesis alterna (H_1). De igual forma, el valor de Z es de -6.154, se ubica en la zona de rechazo de la hipótesis nula; por lo tanto, el DNI electrónico mejora significativamente el índice de tiempo de respuesta en el control de acceso a los sistemas de información en la Superintendencia Nacional de Educación Superior Universitaria, Lima 2021.

Hipótesis específica 3: Índice de disponibilidad de servicio

Formulación de la hipótesis estadística:

H_0: El DNI electrónico no mejora significativamente el índice de disponibilidad de servicio en el control de acceso a los sistemas de información en la Superintendencia Nacional de Educación Superior Universitaria, Lima 2021.

H_1: El DNI electrónico mejora significativamente el índice de disponibilidad de servicio en el control de acceso a los sistemas de información en la Superintendencia Nacional de Educación Superior Universitaria, Lima 2021.

Considerando que el resultado de la prueba de normalidad del índice de disponibilidad de servicio no es normal (ver anexo 7), se aplicó la prueba de Wilcoxon.

Tabla 10

Prueba de Wilcoxon del indicador: Índice de disponibilidad de servicio

	Prueba de rangos con signo de Wilcoxon	
	Z	Sig. Asint. (bilateral)
Índice de disponibilidad de servicio Pretest - Postest	-6,154	,000

Nota: Datos asistido en el Software IBM SPSS v22.

Contrastación de hipótesis:

Para la contrastación de la hipótesis se realizó la prueba de Wilcoxon, se visualiza en la tabla 10 que el valor de significancia es de 0.000 hallándose menor al valor alfa de 0.05 por lo que se rechaza la hipótesis nula (H_0) y se acepta la hipótesis alterna (H_1). De igual forma, el valor de Z es de -6.154, se ubica en la zona de rechazo de la hipótesis nula; por lo tanto, el DNI electrónico mejora significativamente el índice de disponibilidad de servicio en el control de acceso a los sistemas de información en la Superintendencia Nacional de Educación Superior Universitaria, Lima 2021.

V. Discusión

De acuerdo a los resultados obtenidos en la investigación realizada señalan los cambios mostrados en los tres indicadores pertenecientes a la variable dependiente control de acceso a los sistemas de información, después de la implementación de la variable independiente DNI electrónico en la Superintendencia Nacional de Educación Superior Universitaria, Lima 2021

Respecto al indicador índice de accesos no autorizados, en el análisis descriptivo se observó una diferencia en las 50 observaciones realizadas. Asimismo, se visualiza cómo se comporta en la figura 1 del indicador índice de accesos no autorizados antes y después de aplicar el DNI electrónico respecto a los datos conseguidos mediante la guía de observación, por lo tanto, se logra deducir que el Índice de accesos no autorizados mejoró de un 80,69 a un 7,13 veces. En este indicador la mejora se dio en la disminución en un 91,16%. Asimismo, para los datos descriptivos del indicador índice de accesos no autorizados se presentan en la tabla 5, además, en el anexo 8(a) podemos observar la gráfica de la fluctuación de las tomas entre el pre-test y post-test; observándose la mejoría después de implementar el DNI electrónico.

De igual modo, en el análisis inferencial referente a la prueba de normalidad se obtuvo como resultado el p-valor fue menor a 0.05, tanto el resultado para el pre-test es de 0.000 y el post-test es de 0.002, determinado que la distribución de los datos es no normal y se utilizó la contrastación de la prueba de hipótesis no paramétrica de rango de Wilcoxon obteniendo el p-valor igual a 0.000, siendo menor a 0.05 del valor alfa, por lo que se rechazó la hipótesis nula H_0 y se aceptó la hipótesis alterna H_1, concluyéndose que el DNI electrónico mejora significativamente el índice de accesos no autorizados en el control de acceso a los sistemas de información en la Superintendencia Nacional de Educación Superior Universitaria, Lima 2021.

Los resultados contrastan con los antecedentes siguientes: Yañez (2019) con su investigación cuyo objetivo es identificar el dominio de un sistema de identificación facial para el control de acceso; quien confirma que el acceso no autorizado se enfatiza que la aplicación de sistemas de control de acceso que ha reducido el acceso no autorizado en un 3%.

Asimismo, Cao et al (2021) en su investigación cuyo objetivo es diseñar un mecanismo de control de acceso basado en tokens con mecanismo inteligentes con ajuste dinámico de las reglas; confirma el beneficio de un diseño de control de acceso no autorizado y acceso malicioso y resalta la regulación del comportamiento de acceso al cliente.

Del mismo modo, Martínez (2018) con su investigación, cuyo objetivo es implementar un sistema de control de acceso a red y resulta ser muy eficiente y beneficioso a fin de prevenir accesos no autorizados a los servicios de red; de la misma forma Neira (2017) con su investigación afirma que es posible implementar un sistema de control de acceso que identifica por medio del número de DNI, que previene el acceso no autorizado al contenido del chip y recalca la importancia de la iluminación y distancia para la detección.

Ademas, Shantanu et al (2020) con su investigación cuyo objetivo fue proporcionar una básica introducción a la tecnología, descripciones y discutir el surgimiento de IoT; confirma la seguridad de proteger el sistema del acceso no autorizado y de salvaguardar la divulgación no autorizada de la información del sistema.

Alineado con el escenario conceptual del indicador se encuentra Acurio. (2016) que menciona que es acceder de manera no permitida, contra derecho o sin autorización sobre un sistema de información. Asimismo, Arellano y Ochoa (2015) indican que el acceso no autorizado se tiene que evaluar a través de la vulneración de medidas de seguridad. Finalmente, de acuerdo con Gómez (2020) menciona que es una realización de operaciones no autorizadas a una red o sistema informática y estos efectos producen daños en la información.

Respecto al indicador índice de accesos no autorizados, en el análisis descriptivo se observó una diferencia en las 50 observaciones realizadas. Asimismo, se visualiza cómo se comporta en la figura 2 del indicador índice de tiempo de respuesta antes y después de aplicar el DNI electrónico respecto a los datos conseguidos mediante la guía de observación, por lo tanto, se logra deducir que el Índice de tiempo de respuesta mejoró de un 17,29 a un 91,77 veces. En este indicador la mejora se dio en el aumento en un 81,16%. Asimismo, para los datos descriptivos del indicador índice de tiempo de respuesta se presentan en la tabla 6, además, en el anexo 8(b) podemos observar la gráfica de la fluctuación de las tomas entre el pre-test y post-test; observándose la mejoría después de implementar el DNI electrónico.

De igual modo, en el análisis inferencial referente a la prueba de normalidad se obtuvo como resultado el p-valor fue menor a 0.05, tanto el resultado para el pre-test es de 0.000 y el post-test es de 0.003, determinado que la distribución de los datos es no normal y se utilizó la contrastación de la prueba de hipótesis no paramétrica de rango de Wilcoxon obteniendo el p-valor igual a 0.000, siendo menor a 0.05 del valor alfa, por lo que se rechazó la hipótesis nula H_0 y se aceptó la hipótesis alterna H_1, concluyéndose que el DNI electrónico mejora significativamente el índice de tiempo de respuesta en el control de acceso a los sistemas de información en la Superintendencia Nacional de Educación Superior Universitaria, Lima 2021.

Los resultados contrastan con los antecedentes siguientes: Ragesh y Baskaran (2016) con su investigación cuyo objetivo fue analizar la seguridad de su esquema propuesto y su evaluación de desempeño en los sistemas; afirma que un esquema de cifrado aporta al tiempo de respuesta en comparación otros esquemas; en esa misma línea Yueliu et al (2020) con su investigación; menciona que el tiempo en el control de acceso mejora con la implementación de la tecnologia electronica digital.

Alineado con el escenario conceptual del indicador se encuentra a RajSudhakar et al (2021) que mencionan como tiempo transcurrido entre la

activación y la finalización de un trabajo de una tarea. Asimismo, Chydzins y Adamczyk (2020) mencionan como el total de tiempo que un paquete aceptado pasa en el sistema, incluido el tiempo de servicio de este paquete. Finalmente, de acuerdo con Romero (2015) define como la complejidad de factores que se involucran en la calidad del servicio y que brinda una organización o entidad ya sea pública o privada.

Respecto al indicador índice de accesos no autorizados, en el análisis descriptivo se observó una diferencia en las 50 observaciones realizadas. Asimismo, se visualiza cómo se comporta en la figura 3 del indicador índice de disponibilidad de servicio antes y después de aplicar el DNI electrónico respecto a los datos conseguidos mediante la guía de observación, por lo tanto, se logra deducir concluir que el Índice de disponibilidad de servicio mejoró de un 19,50 a un 92,84 veces. En este indicador la mejora se dio en el aumento en un 78,99%. Asimismo, para los datos descriptivos del indicador índice de disponibilidad, se presentan en la tabla 7, además, en el anexo 8(c) podemos observar la gráfica de la fluctuación de las tomas entre el pre-test y post-test; observándose la mejoría después de implementar el DNI electrónico.

De igual modo, en el análisis inferencial referente a la prueba de normalidad se obtuvo como resultado el p-valor fue menor a 0.05, tanto el resultado para el pre-test es de 0.000 y el post-test es de 0.001, determinado que la distribución de los datos es no normal y se utilizó la contrastación de la prueba de hipótesis no paramétrica de rango de Wilcoxon obteniendo el p-valor igual a 0.000, siendo menor a 0.05 del valor alfa, por lo que se rechazó la hipótesis nula H_0 y se aceptó la hipótesis alterna H_1, concluyéndose que el DNI electrónico mejora significativamente el índice de disponibilidad de servicio en el control de acceso a los sistemas de información en la Superintendencia Nacional de Educación Superior Universitaria, Lima 2021.

Asimismo, Espinoza (2018) en su investigación, cuyo objetivo es el desarrollo para la implementación de seguridad inalámbrica en el control de acceso para los

usuarios; muestra que más del 80% se encuentra convencido de la implementación y control en el tráfico inalámbrico para así obtener ventajas en la disponibilidad de servicio.

De igual manera, Rubio y Gómez (2017) en su investigación cuyo objetivo es aprovechar el uso de los certificados digitales que contiene el DNI electrónico, afirma que con la implementación del DNI electrónico beneficia la disponibilidad del servicio para múltiples plataformas para poder hacer uso de los certificados, asimismo, de igual forma Martínez (2018) en su investigación, afirman relevancia para la disponibilidad de servicio continuo para transferencia de información digital electrónicamente.

Alineado con el escenario conceptual del indicador se encuentra Sepulveda y de Jesús (2018) menciona que consiste en la capacidad de cierto componente de configuración o de un servicio TI la cual cumple sus funciones establecidas al momento que lo soliciten. Asimismo, Cevallos (2018) define como el tiempo que dispone para solucionar y atender un servicio o un bien. Finalmente, de acuerdo con Rogel (2018) menciona que es la posibilidad de un servicio o un bien que está presente en el momento que este se lo necesite.

Respecto al objetivo general busca determinar que el DNI electrónico mejora en el control de acceso a los sistemas de información en la Superintendencia Nacional de Educación Superior Universitaria, Lima 2021. Por consiguiente, en el primer indicador índice de accesos no autorizados su comportamiento antes y después de la implementación del DNI electrónico de los datos obtenidos en la guía de observación, por el cual, muestra datos positivos en el índice de accesos no autorizados mejoro de un 80,69 a un 7,13 veces; en este indicador la mejora se dio en la disminución en un 91,16%.

Asimismo, en el segundo indicador índice de tiempo de respuesta su comportamiento antes y después de la implementación del DNI electrónico de los datos obtenidos en la guía de observación, por el cual, muestra datos positivos en el índice de tiempo de respuesta mejoró de un 17,29 a un 91,77 veces; en este indicador la mejora se dio en el aumento en un 81,16%.

Finalmente, el tercer indicador índice de disponibilidad su comportamiento antes y después de la implementación del DNI electrónico de los datos obtenidos en la guía de observación, por el cual, muestra datos positivos en el Índice de disponibilidad de servicio mejoro de un 19,50 a un 92,84 veces; en este indicador la mejora se dio en el aumento en un 78,99%.

Respecto a la Metodología de Investigación utilizada, es un diseño de estudio experimental puro y se pueden utilizar asignaciones aleatorias para verificar la validez interna del experimento enriqueciendo así la investigación. Asimismo, al realizar pruebas pre-test y post-test, es posible medir con mayor precisión los cambios aplicados para interpretar los resultados e identificar las asociaciones de causa y efecto, de la relación directa entre las variables de investigación. Además, se pudo conocer el estado actual del flujo de control de acceso de la Superintendencia Nacional de Educación Superior Universitaria, Lima 2021.

Es importante señalar que el uso del instrumento de las guías de observación favoreció en gran medida la obtención de recolección de datos, ya que estos fueron extraídos en el lugar o en campo de manera inmediata; finalmente, los indicadores establecidos en el trabajo de investigación permitieron conocer que la empresa en estudio se encuentra preocupada por disponer de la información necesaria para la medición de la variable dependiente.

En cuanto a la relevancia social científica, la investigación proporciona la expansión de conocimiento del DNI electrónico en el control de acceso hacia todos los sistemas de información; por otro lado, esta tecnología puede ser utilizada en otras entidades nacionales y privadas.

VI: Conclusiones

Primera: De acuerdo a los resultados obtenidos se determina que el DNI electrónico mejora significativamente el control de acceso a los sistemas de información, en la en la Superintendencia Nacional de Educación Superior Universitaria, en el cual los puntos principales de las mejoras son los indicadores, cómo se puede verificar con el indicador Índice de accesos no autorizados donde la mejora se dio en la disminución en un 91,16%, asimismo el indicador Índice de tiempo de respuesta donde la mejora se dio en el aumento en un 81,16%, por último el indicador Índice de disponibilidad de servicio donde la mejora se dio en el aumento en un 78,99%, en los sistemas de información de la Superintendencia Nacional de Educación Superior Universitaria.

Segunda: En cuanto al primer indicador el Índice de accesos no autorizados, se observó la mejora luego de la implementación del DNI electrónico, donde la mejora se dio en la disminución en un 91,16% en promedio, en la precisión de accesos no autorizados, esta actividad señala que los procedimientos realizados se están ejecutando de forma óptima.

Tercera: Para el segundo indicador el Índice de tiempo de respuesta, se observó la mejora luego de la implementación del DNI electrónico, donde la mejora se dio en el aumento en un 81,16% en promedio, en la precisión del tiempo de respuesta, esta actividad señala que los procedimientos realizados se están ejecutando de forma óptima.

Cuarta: Para el tercer indicador qué es el Índice de disponibilidad de servicio, se observó en la mejora luego de la implementación del DNI electrónico, donde la mejora se dio en el aumento en un 78,99% en promedio, en la precisión de la disponibilidad de servicio, esta actividad señala que los procedimientos realizados se están ejecutando de forma óptima.

VII. Recomendaciones

Primera: Para lograr un sostenimiento y mostrar los resultados positivos en los tres indicadores obtenidos por la presente investigación en la oficina de tecnologías de la información de la Superintendencia Nacional de Educación Superior Universitaria, después de la implementación del DNI electrónico para control de acceso a los sistemas de información, se precisa al jefe de la Oficina de Tecnologías de la Información la implementación del DNI electrónico en todas las aplicaciones utilizadas en la institución, además de la creación de un manual y procedimiento para el óptimo control de acceso.

Segunda: Para mantener la reducción en el indicador Índice de accesos no autorizados, se recomienda al jefe de la Oficina de Tecnologías de la Información un mayor seguimiento al registro de actividades de accesos, además de capacitar a los usuarios finales sobre el uso del DNI electrónico.

Tercera: Para conservar el aumento en cuanto al indicador Índice de tiempo de respuesta, se recomienda al jefe de la Oficina de Tecnologías de la Información hacer mantenimiento de bases de datos y actualización de herramientas, para evitar demoras en el proceso de acceso por medio del DNI electrónico.

Cuarta: Finalmente, para mantener el indicador Índice de disponibilidad de servicio, se recomienda al jefe de la Oficina de Tecnologías de la Información tener un monitoreo para tener exactitud con herramientas que permitan escalar, además ser tolerante a fallas y la flexibilidad tecnológica para sacar el mejor partido a la tecnología utilizada.

REFERENCIAS

Acurio, S. (2016). Acceso no autorizado a sistemas de información. Extraído desde: https://www.oas.org/juridico/spanish/cyb_ecu_delitos_inform.pdf

Arellano, W. y Ochoa, V. (2015). Derechos de privacidad e información en la sociedad de la información y en el entorno TIC. Artículos de revista. Extraído desde: http://www.scielo.org.mx/scielo.php?script=sci_arttext&pid=S1870-21472013000100010

Aqsa, F. Colomo, R. (2018). Security aspects in healthcare information systems: A systematic mapping. Procedia Informática. (v)-138. Extraído de: https://www.sciencedirect.com/science/article/pii/S187705091831634X

Bardeen, M. y Cerpa, N. (2015). Technological Evolution in Society - The Evolution of Mobile Devices. Journal of theoretical and applied electronic commerce research. (v)-10. 1. Extraído de: https://www.scielo.cl/scielo.php?script=sci_arttext&pid=S0718-18762015000100001

Bixter, M. Wendy, A. y Rogers, I. (2018). Enhancing social engagement of older adults through technology. Aging, Technology and Health. Extraído de: https://www.sciencedirect.com/topics/psychology/technological-innovation

Cevallos, J. (2018). Análisis de la calidad de servicio de los locales que se dedican a la venta de computadoras en el centro de mantu. Facultad De Ciencia Administrativas.TESIS Extraído desde: https://repositorio.uleam.edu.ec/bitstream/123456789/1443/1/ULEAM-ADM-0037.pdf

Cao, S. Danga, S. Zhang, Y. Wang, W. y Cheng, N. (2021). A blockchain-based access control and intrusion detection framework for satellite communication systems. Computer Communications. (v)-172. Extraído de: https://www.sciencedirect.com/science/article/pii/S0140366421001250

Coccia, M. (2019). The theory of technological parasitism for the measurement of the evolution of technology and technological forecasting. Technological Forecasting and Social Change. (v)-41. Extraído de: https://www.sciencedirect.com/science/article/abs/pii/S004016251830581X

Chao, L. Debiao, H. Xinyi, H. et, al. (2011). The changing face of electronic ID. Biometric Technology Today. Extraído de: https://www.sciencedirect.com/science/article/abs/pii/S0969476511700145

Chin-Ling, Chen, et, al. (2008). National e-ID card schemes: A European overview. Information Security Technical Report. Extraído de: https://www.sciencedirect.com/science/article/abs/pii/S1363412708000241

Chydzins, A. y Adamczyk, k. (2020). Response time of the queue with the dropping function. Applied Mathematics and Computation. (v)-377. Extraído de: https://www.sciencedirect.com/science/article/pii/S0096300320301338

Covarrubias, G. (2015) ¿Cómo definir la disponibilidad de un servicio?. Grupos de Usuarios de GNU/Linux de Tijuana. Extraído desde: http://www.gultij.org/wp-content/uploads/2015/05/Disponibilidad-de-Servicios-Presentacion-GULTij-Mayo-2015.pdf

Cummings, T. (2001). Closed and Open Systems: Organizational. International Encyclopedia of the Social & Behavioral Sciences. https://www.sciencedirect.com/science/article/pii/B0080430767042212

Espinoza, E. (2018). “Desarrollo e implementación de un sistema de control de acceso a redes inalámbricas mediante RADIUS”. Universidad Nacional Mayor de San Marcos. Facultad de ingeniería electrónica y eléctrica. Extraído de: https://cybertesis.unmsm.edu.pe/bitstream/handle/20.500.12672/10018/Espinoza_ae.pdf?sequence=1&isAllowed=y

Filippos, A. Euripides, G. Estelios, S. y Bessis, N. (2018). A physical access control system on the cloud. Procedia Computer Science. (v)-130. Extraído de: https://www.sciencedirect.com/science/article/pii/S1877050918303983

Galindo H. (2020). Estadísticos para no estadísticos, Una guía básica sobre la metodología cuantitativa de trabajos académicos. Economia, Organización y Ciencias Sociales. 1, 3-9. extraido de: https://www.3ciencias.com/wp-content/uploads/2020/03/Estad%C3%ADstica-para-no-estad%C3%ADsticos-Una-gu%C3%ADa-b%C3%A1sica-sobre-la-metodolog%C3%ADa-cuantitativa-de-trabajos-acad%C3%A9micos-2.pdf

Gliem, J. y Gliem, R. (2003). Calculating, Interpreting, and Reporting Cronbach’s Alpha Reliability Coefficient for Likert-Type Scales. Midwest Research to Practice Conference in Adult, Continuing, and Community Education. Extraido de: https://scholarworks.iupui.edu/handle/1805/344

Gómez, A. (2020) Seguridad informática y protección de datos. Extraído desde: https://www.ceupe.com/blog/seguridad-informatica-y-proteccion-de-datos.html

Gupta B. y Megha Q. (2018). An identity based access control and mutual authentication framework for distributed cloud computing services in IoT environment using smart cards. Procedia Computer Science. Extraido de: https://www.sciencedirect.com/science/article/pii/S1877050918309190

Hans, J. (1994). Applications of general systems theory to the development of an adjustable tutorial software machine. Computers & Education. (v)-22. Extraído de: https://www.sciencedirect.com/science/article/pii/0360131594900086

Hernández, R. Fernández, C. y Baptista, M. (2014). Metodología de la investigación. Obtenido de: https://www.uca.ac.cr/wp-content/uploads/2017/10/Investigacion.pdf

Lapiedra, R. Devece, C. y Guiral, J. (2015). Introducción a la gestión de sistemas informáticos en la empresa [en línea]. 1a ed. México: Colección sapientía. 2015. Extraído desde: https://libros.metabiblioteca.org/handle/001/193

Laudon, C. y Laudon, P. (2016). Sistemas de información Gerencial, Pearson Educación, México. 14ª ed. 2016. Extraído desde: https://juanantonioleonlopez.files.wordpress.com/2017/08/sistemas-de-informacic3b3n-gerencial-12va-edicic3b3n-kenneth-c-laudon.pdf

Loor, J. Parra, T. Frodeman, C. Bertalanffy, L. (2019). teoría general de los sistemas. Universidad Técnica de Manabí (UTM). Extraído desde: https://www.researchgate.net/publication/337683271_TEORIA_GENERAL_DE_SISTEMA

Martinez, E. (2018). Implementación del DNIe en la Comisión de Presupuesto del Congreso de la Republica. Repositorio digital institucional. Universidad César Vallejo. Extraído de: https://repositorio.ucv.edu.pe/handle/20.500.12692/15311

Martínez, J. (2018). Implementación de un sistema de control de acceso a red en la empresa sima-Chimbote. Universidad Católica los Ángeles de Chimbote. Facultad de ingeniería de sistemas. Extraído de: http://repositorio.uladech.edu.pe/bitstream/handle/123456789/3054/ACCESO_CONTROL_MARTINEZ_CABRERA_BENIGNO.pdf?sequence=1&isAllowed=y

Neira, E. (2017). “Sistema de lectura automática del número de DNI utilizando visión artificial”. Universidad Nacional de Piura. Facultad de Ciencias. Extraído de: http://repositorio.unp.edu.pe/bitstream/handle/UNP/1757/CIE-NEI-MIJ-2017.pdf?sequence=1&isAllowed=y

Olakanmi, O. y Dunun, K. (2020). FEACS: A fog enhanced expressible access control scheme with secure services delegation among carers in E-health systems. Internet of Things. (v)-12. Extraído de: https://www.sciencedirect.com/science/article/abs/pii/S2542660520301098

PAE. (2016). Formatos de firma. Portal Administración Electrónica. Gobierno de España. Extraído desde: https://firmaelectronica.gob.es/Home/Ciudadanos/Formatos-Firma.Html#formatos_firma

Porras A. y Jaime C. (2016). Comparación de Pruebas de Normalidad Multivariada. REIRE. Revista Dialnet Plus. V. 77, 141-146. extraido de: https://dialnet.unirioja.es/servlet/articulo?codigo=6171231

Ragesh G. y Baskaran D. (2016). Cryptographically Enforced Data Access Control in Personal Health Record Systems. Procedia Technology. Extraido de: https://www.sciencedirect.com/science/article/pii/S2212017316304819

RajSudhakar, D. Albers, K.y Slomkab, F. (2021).Generalized and Scalable Offset-Based Response Time Analysis of Fixed Priority Systems. Journal of Systems Architecture. (v)-112. Extraído de: https://www.sciencedirect.com/science/article/pii/S1383762120301417

Rezende, D. y Abreu, A. (2010). Tecnologia da Informação Aplicada a Sistemas de Informação Empresariais: o papel estratégico da informação e dos sistemas de informação nas empresas: Ed. Atlas. São Paulo. Obtenido de https://edisciplinas.usp.br/pluginfile.php/5608406/mod_resource/content/1/Teoria%20Geral%20dos%20Sistemas%20e%20os%20Sistemas%20de%20Informac%CC%A7a%CC%83o%20-%20Portal%20Educac%CC%A7a%CC%83o.pdf

Rogel, J. (2018) (QUALITY OF SERVICE AND CUSTOMER SATISFACTION: KEY BINOMIAL IN TRAVEL AGENCIES IN ECUADOR). TESIS. Extraído desde: http://www.postgradovipi.50webs.com/archivos/memoralia/2018-I/ARTICULO15.pdf

Romero, M. (2015) La satisfacción del cliente http://bibing.us.es/proyectos/abreproy/3966/fichero/1%252F2.pdf

Romero, M. y Figueroa, G. (2018) INTRODUCCIÓN A LA SEGURIDAD INFORMÁTICA Y EL ANÁLISIS DE VULNERABILIDADES. Tesis. Extraído desde: https://www.3ciencias.com/wp-content/uploads/2018/10/Seguridad-inform%C3%A1tica.pdf

Rubio, J. (2017). Implementación de un servicio de autenticación y firma empleando el DNI electrónico. Escuela tecina superior de ingeniería y sistema de telecomunicación. Departamento de ingeniería telemática y electrónica. España-Madrid. Extraído de: http://oa.upm.es/51781/

Shantanu, P. Hitchens, M. y Vijay, V. (2020). Access control for Internet of Things—enabled assistive technologies: an architecture, challenges and requirements. Assistive Technology for the Elderly. Extraido de: https://www.sciencedirect.com/science/article/pii/B9780128185469000014

Sepulveda, I. y de jesus, A. (2018). Servicio al cliente e integración del marketing mix de servicios. Artículo de revista.

http://www.cucea.udg.mx/sites/default/files/documentos/adjuntos_pagina/servicio_al_cliente_e_integracion_del_marketing_mix_de_servicios.pdf

Sieniutycz, S. (2020). Chapter 1 - Systems science vs cybernetics. Complexity and Complex Thermo-Economic Systems. Extraído de: https://www.sciencedirect.com/science/article/pii/B9780128185940000015

Teece, J. (2010). Chapter 16 - Technological Innovation and the Theory of the Firm: The Role of Enterprise-Level Knowledge, Complementarities, and (Dynamic) Capabilities. Handbook of the Economics of Innovation. (v)-1. Extraído de: https://www.sciencedirect.com/science/article/pii/S0169721810010166

Tidd, J. Bessant, J. Pavitt, K. (2005). Managing innovation: integrating technological, market and organizational change: New York. John Wiley & Sons. Obtenido de https://www.revistas.usp.br/rai/article/view/100344/98997

Tim Weilkiens, L. (2007). General System Theory. Military Applications of Complex Systems. Extraído de: https://www.sciencedirect.com/topics/computer-science/general-system-theory

Torres, I. Pesántez, S. Guapacaza, D. y Montesdeoca, P. (2019) La innovación tecnológica y la calidad pedagógica de los docentes de la unidad educativa Olmedo, Ecuador, 2019. Extraído desde: https://repositorio.ucv.edu.pe/handle/20.500.12692/42677

Ummer I. y Ajaz H. (2020). Secure and scalable access control protocol for IoT environment. Internet of Things. Extraido de: https://www.sciencedirect.com/science/article/pii/S2542660520301232

Valderrama, S. (2013). PASOS PARA ELABORAR PROYECTOS DE INVESTIGACIÓN CIENTÍFICA. Extraído desde: http://www.sancristoballibros.com/libro/pasos-para-elaborar-proyectos-de-investigacion-cientifica_45757

Yañez, M. (2019). Sistema de reconocimiento facial para el control de acceso de estudiantes a los laboratorios de la FIIS-UNAC, 2019. Universidad César Vallejo. Facultad de ingeniería de sistemas. Extraído de: https://repositorio.ucv.edu.pe/handle/20.500.12692/44310

Yrivarren, J. (2015). Gobierno digital, avances y desafíos. encuentro del sector público. Extraído desde: https://sgp.pcm.gob.pe/wp-content/uploads/2015/10/JORGE_YRIVARREN_RENIEC.pdf

Yua, J. yingJi, H. Song, Q. y Zhoubca, L. (2021). Design and implementation of business access control in new generation power grid dispatching and control system. Procedia Computer Science. (v)-183. Extraído de: https://www.sciencedirect.com/science/article/pii/S1877050921006025

YueLiu, Q. Shiping, C. Qiang, Q. Et al. (2020). Capability-based IoT access control using blockchain. Digital Communications and Networks. Extraido de: https://www.sciencedirect.com/science/article/pii/S2352864820302844

ANEXOS

Anexo 1: Matriz de Consistencia

TÍTULO: DNI electrónico en la mejora de la control de acceso a los sistemas de información en la Superintendencia Nacional de Educación Superior Universitaria, Lima 2021

AUTOR: Victor Alejandro Arroyo Castro

PROBLEMA	OBJETIVOS	HIPÓTESIS	VARIABLES E INDICADORES	
Problema principal: ¿De qué manera el DNI electrónico mejora en el control de acceso a los sistemas de información en la Superintendencia Nacional de Educación Superior Universitaria, Lima 2021? **Problemas específicos:** PE1: ¿De qué manera el DNI electrónico mejora el índice de accesos no autorizados en el control de acceso a los sistemas de información en la Superintendencia Nacional de Educación	**Objetivo principal:** Determinar que el DNI electrónico mejora en el control de acceso a los sistemas de información en la Superintendencia Nacional de Educación Superior Universitaria, Lima 2021 **Objetivos específicos:** OE1: Determinar que el DNI electrónico mejora el índice de accesos no autorizados en el control de acceso a los sistemas de información en la Superintendencia Nacional de Educación Superior Universitaria, Lima 2021	**Hipótesis principal:** El DNI electrónico mejora significativamente en el control de acceso a los sistemas de información en la Superintendencia Nacional de Educación Superior Universitaria, Lima 2021 **Hipótesis específicas:** HE1: El DNI electrónico mejora significativamente el índice de accesos no autorizados en el control de acceso a los sistemas de información en la Superintendencia Nacional de Educación Superior Universitaria, Lima 2021	**Variable Independiente: DNI electrónico** **Variable Dependiente: Control de acceso a los sistemas de información**	
			Indicadores	**Unidad de medida**
			Índice de accesos no autorizados	Porcentaje
			Índice de tiempo de respuesta	Porcentaje
			Índice de disponibilidad de servicio	Porcentaje

TÍTULO: DNI electrónico en la mejora de la control de acceso a los sistemas de información en la Superintendencia Nacional de Educación Superior Universitaria, Lima 2021

AUTOR: Victor Alejandro Arroyo Castro

PROBLEMA	OBJETIVOS	HIPÓTESIS	VARIABLES E INDICADORES
Superior Universitaria, Lima 2021?			
PE2: ¿De qué manera el DNI electrónico mejora el índice de tiempo de respuesta en el control de acceso a los sistemas de información en la Superintendencia Nacional de Educación Superior Universitaria, Lima 2021?	OE2: Determinar que el DNI electrónico mejora el índice de tiempo de respuesta en el control de acceso a los sistemas de información en la Superintendencia Nacional de Educación Superior Universitaria, Lima 2021	HE2: El DNI electrónico mejora significativamente el índice de tiempo de respuesta en el control de acceso a los sistemas de información en la Superintendencia Nacional de Educación Superior Universitaria, Lima 2021	
PE3: ¿De qué manera el DNI electrónico mejora el índice de disponibilidad de servicio en el control de acceso a los sistemas de información en la Superintendencia Nacional de Educación Superior Universitaria, Lima 2021?	OE3: Determinar que el DNI electrónico mejora el índice de disponibilidad de servicio en el control de acceso a los sistemas de información en la Superintendencia Nacional de Educación Superior Universitaria, Lima 2021	HE3: El DNI electrónico mejora significativamente el índice de disponibilidad de servicio en el control de acceso a los sistemas de información en la Superintendencia Nacional de Educación Superior Universitaria, Lima 2021	

Metodología

TIPO Y DISEÑO	POBLACIÓN Y MUESTRA	TÉCNICAS E INSTRUMENTOS	ESTADÍSTICA POR UTILIZAR
Tipo: Aplicada **Diseño:** Experimental Puro.	**Población:** 50 registros **Muestreo:** Probabilístico del tipo Aleatorio simple	**Técnicas:** Observación **Instrumentos:** Guías de observación	**Descriptiva**: Para el análisis descriptivo, se implementará a través de tablas y figuras, los cuales serán explicados con medidas de tendencia central usando la media, además se realizará la interpretación o lectura de cada indicador, todo esto ayudará a tener una mejor visualización de manera estructurada, comprensible y sencilla de los datos numéricos. **Inferencial**: Para el análisis inferencial, se comprobará la normalidad de los datos obtenidos a través de la prueba Test de Shapiro Wilk; Asimismo, se usará para la comprobación de la hipótesis la prueba no paramétrica de los rangos con signo de Wilcoxon, está proviene de la prueba paramétrica t para muestras relacionadas y la prueba t Student (para distribución normal)

Anexo 2: Matriz de Operacionalización de Variables

TÍTULO**:** DNI electrónico en la mejora de la control de acceso a los sistemas de información en la Superintendencia Nacional de Educación Superior Universitaria, año 2021

AUTOR: Victor Alejandro Arroyo Castro

INDICADOR	DEFINICIÓN	INSTRUMENTO	UNIDAD DE MEDIDA	FÓRMULA
Índice de accesos no autorizados	Acurio. (2016) Indica el acceso no autorizado a un sistema informático, se refiere en acceder de manera no permitida, contra derecho o sin autorización sobre un sistema de información.	Guía de observación	Porcentaje	$X = \frac{Nº\ de\ accesos\ no\ autorizados}{Nº\ total\ de\ accesos} x\ 100$
Índice de tiempo de respuesta	RajSudhakar, Albers y Slomkab (2021). Refieren al tiempo de respuesta que es el tiempo transcurrido entre la activación y la finalización de un trabajo de una tarea.	Guía de observación	Porcentaje	$X = \frac{Nº\ de\ tiempo\ de\ respuesta\ en\ los\ acceso}{Nº\ de\ tiempo\ total\ de\ accesos} x\ 100$
Índice de disponibilidad de servicio	Sepulveda & De Jesus (2018), La disponibilidad de servicios consiste en la capacidad de cierto componente de configuración o de un servicio TI la cual cumple sus funciones establecidas al momento que lo soliciten.	Guía de observación	Porcentaje	$X = \frac{Nº\ de\ accesos\ atendidos}{Nº\ total\ de\ accesos\ solicitados} x\ 100$

Anexo 3: Instrumento de Recolección de Datos

Guía de observación N° 1. Índice de accesos no autorizados

Guía de observación de medición del indicador Índice de accesos no autorizados					
Investigador:			Victor Alejandro Arroyo Castro		
Proceso observado:			Control de acceso a los sistemas de información		
Pre-Test					
N° de Obs.	Toma	Fecha	Nº de accesos no autorizados	Nº total de accesos	$X = \frac{Nº\ de\ accesos\ no\ autorizados}{Nº\ total\ de\ accesos}\ x\ 100$
1					
2					
3					
4					
5					
6					
N					

Guía de observación de medición del indicador Índice de accesos no autorizados					
Investigador:			Victor Alejandro Arroyo Castro		
Proceso observado:			Control de acceso a los sistemas de información		
Post-Test					
N° de Obs.	Toma	Fecha	Nº de accesos no autorizados	Nº total de accesos	$X = \frac{Nº\ de\ accesos\ no\ autorizados}{Nº\ total\ de\ accesos}\ x\ 100$
1					
2					
3					
4					
5					
6					
N					

Guía de observación N° 2. Índice de tiempo de respuesta

Guía de observación de medición del indicador Índice de tiempo de respuesta					
Investigador:			Victor Alejandro Arroyo Castro		
Proceso observado:			Control de acceso a los sistemas de información		
Pre-Test					
N° de Obs.	Toma	Fecha	Nº de tiempo de respuesta en los accesos	Nº de tiempo total de accesos	$X = \frac{Nº\ de\ tiempo\ de\ respuesta\ en\ los\ acceso}{Nº\ de\ tiempo\ total\ de\ accesos} x\ 100$
1					
2					
3					
4					
5					
6					
N					

Guía de observación de medición del indicador Índice de tiempo de respuesta					
Investigador:			Victor Alejandro Arroyo Castro		
Proceso observado:			Control de acceso a los sistemas de información		
Post-Test					
N° de Obs.	Toma	Fecha	Nº de tiempo de respuesta en los accesos	Nº de tiempo total de accesos	$X = \frac{Nº\ de\ tiempo\ de\ respuesta\ en\ los\ acceso}{Nº\ de\ tiempo\ total\ de\ accesos} x\ 100$
1					
2					
3					
4					
5					
6					
N					

Guía de observación N° 3. Índice de disponibilidad de servicio

Guía de observación de medición del indicador Índice de disponibilidad de servicio					
Investigador:			Victor Alejandro Arroyo Castro		
Proceso observado:			Control de acceso a los sistemas de información		
Pre-Test					
N° de Obs.	Toma	Fecha	Nº de accesos atendidos	Nº total de accesos solicitados	$X = \frac{Nº\ de\ accesos\ atendidos}{Nº\ total\ de\ accesos\ solicitados} x\ 100$
1					
2					
3					
4					
5					
6					
N					

Guía de observación de medición del indicador Índice de disponibilidad de servicio					
Investigador:			Victor Alejandro Arroyo Castro		
Proceso observado:			Control de acceso a los sistemas de información		
Post-Test					
N° de Obs.	Toma	Fecha	Nº de accesos atendidos	Nº total de accesos solicitados	$X = \frac{Nº\ de\ accesos\ atendidos}{Nº\ total\ de\ accesos\ solicitados} x\ 100$
1					
2					
3					
4					
5					
6					
N					

Anexo 4: Certificado de Validación del Instrumento de Recolección de Datos

Validación del Experto N°1

CERTIFICADO DE VALIDEZ DE CONTENDO DEL INSTRUMENTO

VARIABLE: CONTROL DE ACCESO A LOS SISTEMAS DE INFORMACIÓN

Nº	INDICADORES	Claridad[1]		Pertinencia[2]		Relevancia[3]		Sugerencias
		Si	No	Si	No	Si	No	
1	Índice de accesos no autorizados $X = \frac{Nº\ de\ accesos\ no\ autorizados}{Nº\ total\ de\ accesos}\ x\ 100$	X		X		X		
2	Índice de tiempo de respuesta $X = \frac{Nº\ de\ tiempo\ de\ respuesta\ en\ los\ acceso}{Nº\ de\ tiempo\ total\ de\ accesos}\ x\ 100$	X		X		X		
3	Índice de disponibilidad de servicio $X = \frac{Nº\ de\ tiempo\ de\ respuesta\ en\ los\ acceso}{Nº\ total\ de\ accesos}\ x\ 100$	X		X		X		

Observaciones (precisar si hay suficiencia):_____

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

17 de Mayo del 2021

Apellidos y nombres del juez evaluador: RAMIREZ JARAMILLO HUMBERT JASMIN **DNI: 46830084**

Especialista: Metodólogo [ ] **Temático [X]**

Grado: Maestro [X] **Doctor [ ]**

Firma del Experto Informante

[1] **Claridad:** Se entiende sin dificultad alguna el enunciado del ítem, es conciso, exacto y directo
[2] **Pertinencia:** Si el ítem pertenece a la dimensión.
[3] **Relevancia:** El ítem es apropiado para representar al componente o dimensión específica del constructo

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

Validación del Experto N°2

CERTIFICADO DE VALIDEZ DE CONTENDO DEL INSTRUMENTO

VARIABLE: CONTROL DE ACCESO A LOS SISTEMAS DE INFORMACIÓN

Nº	INDICADORES	Claridad[1]		Pertinencia[2]		Relevancia[3]		Sugerencias
		Si	No	Si	No	Si	No	
1	Índice de accesos no autorizados $X = \frac{Nº\ de\ accesos\ no\ autorizados}{Nº\ total\ de\ accesos}\ x\ 100$	X		X		X		
2	Índice de tiempo de respuesta $X = \frac{Nº\ de\ tiempo\ de\ respuesta\ en\ los\ acceso}{Nº\ de\ tiempo\ total\ de\ accesos}\ x\ 100$	X		X		X		
3	Índice de disponibilidad de servicio $X = \frac{Nº\ de\ tiempo\ de\ respuesta\ en\ los\ acceso}{Nº\ total\ de\ accesos}\ x\ 100$	X		X		X		

Observaciones (precisar si hay suficiencia):_____

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

17 de Mayo del 2021

Apellidos y nombres del juez evaluador: VERA NUÑEZ GRISELDA GLADYS **DNI: 10095653**

Especialista: Metodólogo [ ] **Temático [X]**

Grado: Maestro [ ] **Doctor [X]**

[1] **Claridad:** Se entiende sin dificultad alguna el enunciado del ítem, es conciso, exacto y directo
[2] **Pertinencia:** Si el ítem pertenece a la dimensión.
[3] **Relevancia:** El ítem es apropiado para representar al componente o dimensión específica del constructo

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

Firma del Experto Informante

Validación del Experto N°3

CERTIFICADO DE VALIDEZ DE CONTENDO DEL INSTRUMENTO

VARIABLE: CONTROL DE ACCESO A LOS SISTEMAS DE INFORMACIÓN

Nº	INDICADORES	Claridad[1]		Pertinencia[2]		Relevancia[3]		Sugerencias
		Si	No	Si	No	Si	No	
1	Índice de accesos no autorizados $X = \frac{Nº\ de\ accesos\ no\ autorizados}{Nº\ total\ de\ accesos}\ x\ 100$	X		X		X		
2	Índice de tiempo de respuesta $X = \frac{Nº\ de\ tiempo\ de\ respuesta\ en\ los\ acceso}{Nº\ de\ tiempo\ total\ de\ accesos}\ x\ 100$	X		X		X		
3	Índice de disponibilidad de servicio $X = \frac{Nº\ de\ tiempo\ de\ respuesta\ en\ los\ acceso}{Nº\ total\ de\ accesos}\ x\ 100$	X		X		X		

Observaciones (precisar si hay suficiencia):__SUFICIENTE_____

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

29 de mayo del 2021

Apellidos y nombres del juez evaluador: VISURRAGA AGÜERO JOEL MARTÍN DNI: 10192315

Especialista: Metodólogo [X] Temático [X]

Grado: Maestro [ ] Doctor [X]

[1] **Claridad:** Se entiende sin dificultad alguna el enunciado del ítem, es conciso, exacto y directo
[2] **Pertinencia:** Si el ítem pertenece a la dimensión.
[3] **Relevancia:** El ítem es apropiado para representar al componente o dimensión específica del constructo
Nota: Suficiencia, se dice suficiencia cuando los ítems planteados son suficientes para medir la dimensión

Dr. Joel Martin Visurraga Agüero

Anexo 5: Base de datos

	Indicador 1		Indicador 2		Indicador 3	
	I1PreTest	I1PostTest	I2PreTest	I2PostTest	I3PreTest	I3PostTest
1	87,50	7,88	13,15	88,78	14,14	98,76
2	86,44	4,76	11,55	81,70	20,13	91,77
3	77,36	0,64	29,60	94,12	20,82	87,32
4	87,77	16,57	14,35	91,46	11,55	93,81
5	86,19	2,35	30,66	90,27	11,80	84,06
6	74,53	4,91	27,97	83,09	44,49	97,59
7	70,00	7,70	16,53	84,23	11,91	99,12
8	83,19	0,79	30,76	83,85	27,39	83,93
9	80,00	3,19	14,09	98,14	19,70	95,97
10	68,78	1,84	14,63	92,83	22,50	87,98
11	77,86	7,99	10,87	99,82	19,56	92,25
12	83,79	10,87	8,38	86,16	13,88	99,21
13	84,07	3,27	9,59	91,76	42,78	89,58
14	85,69	8,35	33,33	94,58	11,00	85,45
15	74,81	7,70	12,52	91,47	32,87	100,00
16	87,53	8,70	8,13	83,40	22,92	82,88
17	73,30	0,85	7,00	84,52	18,80	99,68
18	85,50	6,36	12,04	89,59	12,72	99,64
19	77,74	3,00	35,41	98,50	11,91	99,16
20	76,08	9,60	22,15	86,16	13,87	82,90
21	88,73	0,64	15,82	84,53	14,48	84,32
22	71,30	10,77	16,24	91,98	24,49	95,05
23	84,66	2,75	30,72	97,97	18,72	90,36
24	86,53	8,40	13,44	96,19	23,36	95,24
25	83,66	5,64	9,42	99,30	11,96	99,13
26	85,41	14,43	21,46	83,69	19,91	85,48
27	88,52	17,23	8,45	99,76	19,44	91,25
28	77,78	1,83	9,99	85,44	14,85	93,25
29	55,65	0,90	8,22	99,24	13,96	98,54
30	83,41	9,93	14,78	99,17	27,02	99,54
31	87,53	8,44	12,40	90,36	10,78	94,41
32	84,52	1,62	24,88	90,19	24,46	84,14
33	61,85	4,60	11,87	91,89	18,96	87,39
34	79,52	0,87	26,49	96,81	27,01	84,34
35	86,98	8,67	14,97	96,77	12,16	94,82
36	74,17	6,95	21,64	99,11	23,94	93,34

37	78,19	0,49	9,55	85,51	31,95	90,96
38	80,45	8,74	10,66	99,20	14,86	96,42
39	73,22	14,21	11,82	99,08	12,55	99,03
40	82,52	17,80	13,18	86,75	18,55	92,41
41	83,53	6,22	16,36	88,27	36,15	99,37
42	85,77	21,30	23,44	93,42	16,65	99,72
43	85,25	0,87	13,46	95,21	18,15	94,22
44	79,97	11,40	15,70	88,51	21,85	99,79
45	81,88	6,83	12,69	91,66	13,57	94,05
46	86,55	20,03	39,63	98,35	15,43	83,09
47	88,89	4,52	12,84	94,29	14,52	95,38
48	87,90	10,61	14,76	84,07	17,21	89,95
49	75,23	9,40	18,01	99,29	13,03	95,35
50	76,86	3,19	29,12	88,12	20,26	90,38

Anexo 6: Autorización de la investigación

SUNEDU
Firmado Digitalmente por: TORRES RENGIFO Lizandro FAU 20600044975 soft
Motivo: Doy V°B°
Fecha: 06/07/2021 13:23:26

SUNEDU
Firmado Digitalmente por: BRINGAS MASGO Isaac Ernesto FAU 20600044975 soft
Motivo: Soy el autor del documento
Fecha: 06/07/2021 17:29:17

PERÚ | Ministerio de Educación | Superintendencia Nacional de Educación Superior Universitaria | Secretaría General | Oficina de Tecnologías de la Información

"Decenio de la Igualdad de Oportunidad para Mujeres y Hombres"
"Año del Bicentenario del Perú: 200 años de Independencia"

Lima, 06 de julio de 2021

CARTA N° 003- 2021-SUNEDU-03-09

Señor
Victor Alejandro Arroyo Castro
Calle Aries 1143 COOP. Virgen del Rosario Los Olivos - Lima
victorarroyocastro@gmail.com

ASUNTO : **Solicitud de permiso para realizar investigación académica.**

Referencia : **RTD N° 031620-2021-SUNEDU-TD (Carta 001-2021-VAAC)**

Tengo el agrado de dirigirme a usted, en atención a su solicitud de permiso para realizar investigación académica en el marco de la investigación titulada **"DNI ELECTRÓNICO EN LA MEJORA DEL CONTROL DE ACCESO A LOS SISTEMAS DE INFORMACIÓN EN LA SUPERINTENDENCIA NACIONAL DE EDUCACIÓN SUPERIOR UNIVERSITARIA, LIMA 2021",** del programa de Maestría en Ingeniería de Sistemas con mención en Tecnologías de la Información de la Universidad Cesar Vallejo.

Al respecto, le comunicamos que se le estará brindando las facilidades para acceder a la información requerida siempre que la misma no esté protegida por la Ley N.° 29733, Ley de Protección de Datos Personales y su reglamento. Asimismo, siempre que no esté catalogada como información confidencial o reservada como parte de los procesos internos de la entidad; o sea parte de los procesos de contrataciones en el marco de la Ley N° 30225, Ley de Contrataciones del Estado, su reglamento y modificatorias.

Sin otro particular, reciba un cordial saludo,

DOCUMENTO FIRMADO DIGITALMENTE
ISAAC ERNESTO BRINGAS MASGO
JEFE
OFICINA DE TECNOLOGIAS DE LA INFORMACION
SUPERINTENDENCIA NACIONAL DE EDUCACIÓN
SUPERIOR UNIVERSITARIA - SUNEDU

IEBM/cjlc

Anexo 7: Prueba de Normalidad

Para la presente investigación adoptamos como base a los autores Porras y Jaime (2016) y Galindo (2020) quienes señalan utilizar la prueba de Shapiro-Wilk, debido a que el número de observaciones recolectadas es como máximo 50; esta prueba se aplicó mediante el software IBM SPSS v22, con un nivel de confianza del 95%.
A continuación, se describen los resultados de las pruebas de normalidad de los respectivos indicadores: Índice de accesos no autorizados, Índice de tiempo de respuesta y Índice de disponibilidad de servicio antes y después de implementar el DNI electrónico.

Pruebas de normalidad del indicador: Índice de accesos no autorizados

Formulación de hipótesis estadística:

H_0: Los datos del indicador Índice de accesos no autorizados presentan una distribución normal.

H_1: Los datos del indicador Índice de accesos no autorizados no presentan una distribución normal.

Tabla 1

Prueba de normalidad del indicador: Índice de accesos no autorizados

	Shapiro-Wilk		
	Estadístico	gl	Sig.
Índice de accesos no autorizados – Pre-Test	0,882	50	0,000
Índice de accesos no autorizados – Post-Test	0,921	50	0,002

Nota: Datos realizados en el Software IBM SPSS v22

En la tabla 8, los resultados alcanzados en la prueba reflejaron que el valor de significancia de la muestra del indicador Índice de accesos no autorizados antes fue 0.000 y después fue 0.002 cuyos valores son menores al error asumido de 0.05 entonces se rechaza la hipótesis nula, deduciendo que el indicador no se distribuye normalmente.

Pruebas de normalidad del indicador: Índice de tiempo de respuesta

Formulación de hipótesis estadística:

H_0: Los datos del indicador Índice de tiempo de respuesta presentan una distribución normal.

H_1: Los datos del indicador Índice de tiempo de respuesta no presentan una distribución normal.

Tabla 2

Prueba de normalidad del indicador: Índice de tiempo de respuesta

	Shapiro-Wilk		
	Estadístico	gl	Sig.
Índice de tiempo de respuesta – Pre-Test	0,876	50	0,000
Índice de tiempo de respuesta – Post-Test	0,923	50	0,003

Nota: Datos realizados en el Software IBM SPSS v22

En la tabla 9, los resultados los resultados alcanzados en la prueba reflejaron que el valor de significancia de la muestra del indicador Índice de tiempo de respuesta antes fue 0.000 y después fue 0.003 cuyos valores son menores al error asumido de 0.05 entonces se rechaza la hipótesis nula, deduciendo que el indicador no se distribuye normalmente.

Pruebas de normalidad del indicador: Índice de disponibilidad de servicio

H_0: Los datos del indicador Índice de disponibilidad de servicio presentan una distribución normal.

H_1: Los datos del indicador Índice de disponibilidad de servicio no presentan una distribución normal.

Tabla 3

Prueba de normalidad del indicador: Índice de disponibilidad de servicio

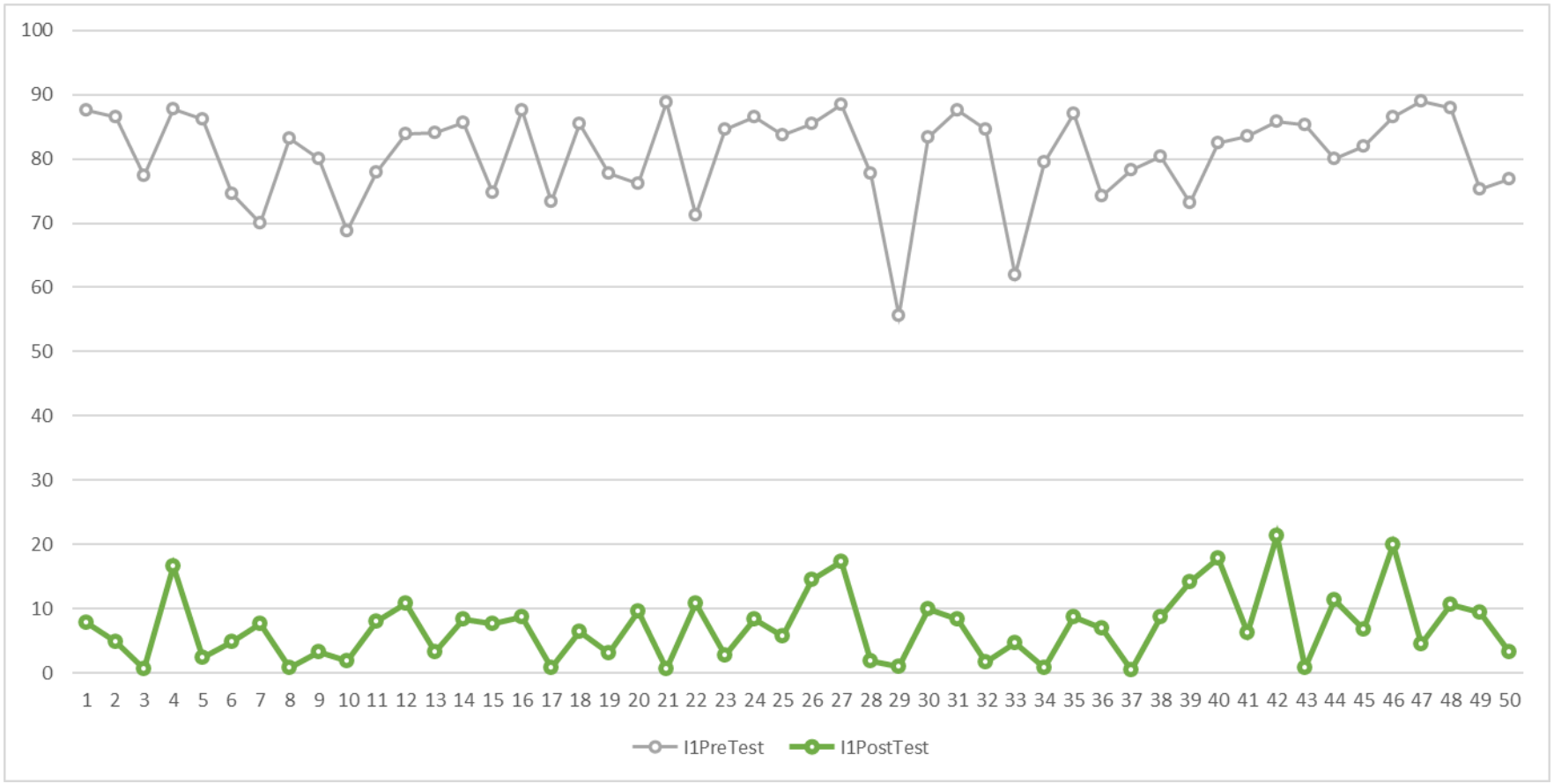
	Shapiro-Wilk		
	Estadístico	gl	Sig.
Índice de disponibilidad de servicio – Pre-Test	0,862	50	0,000
Índice de disponibilidad de servicio – Post-Test	0,908	50	0,001

Nota: Datos realizados en el Software IBM SPSS v22

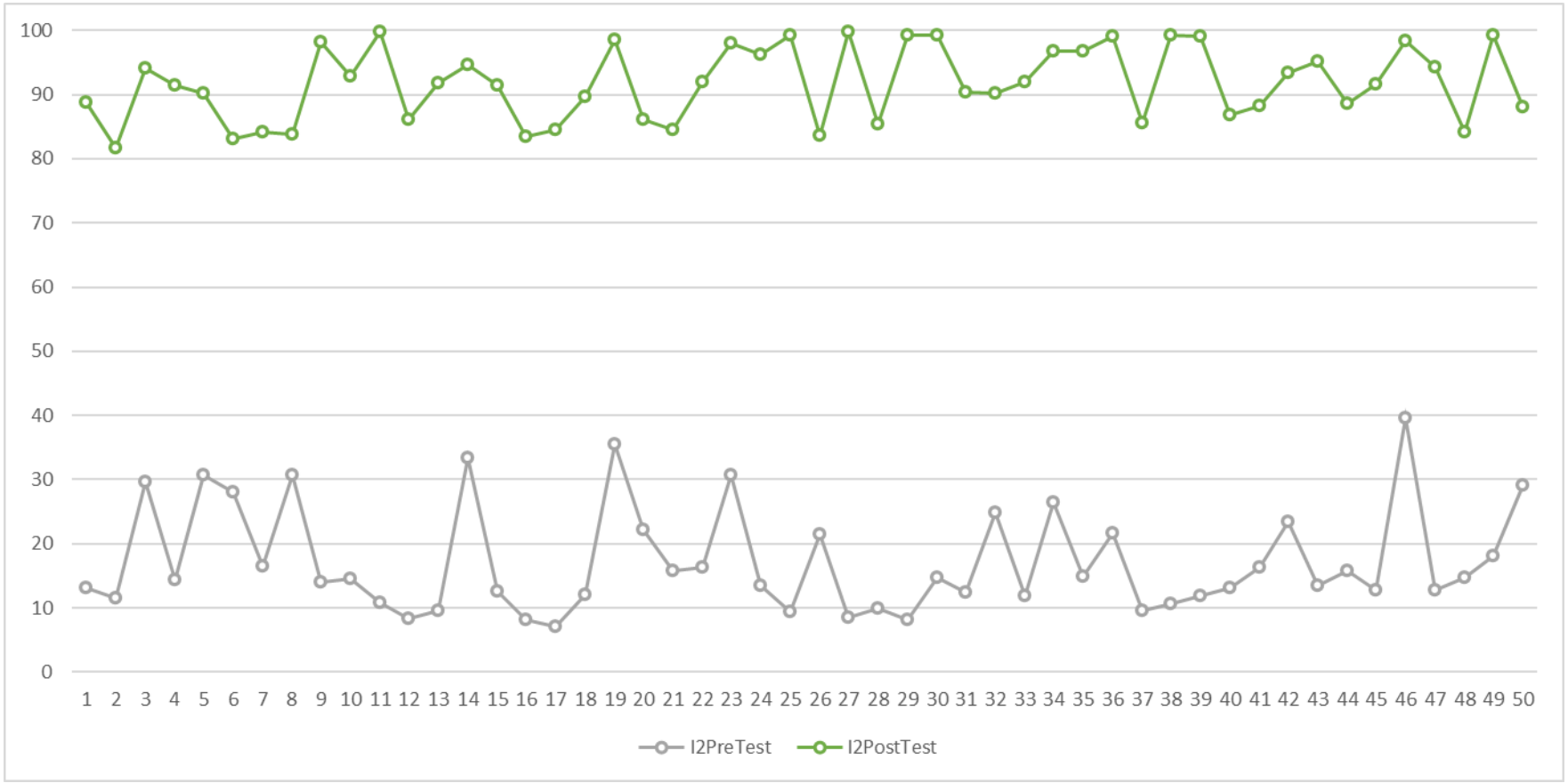
En la tabla 10, los resultados los resultados alcanzados en la prueba reflejaron que el valor de significancia de la muestra del indicador Índice de disponibilidad de servicio antes fue 0.000 y después fue 0.001 cuyos valores son menores al error asumido de 0.05 entonces se rechaza la hipótesis nula, deduciendo que el indicador no se distribuye normalmente.

Anexo 8: Comportamiento de las medias descriptivas

a) Indicador 1: Índice de accesos no autorizados



b) Indicador 2: Índice de tiempo de respuesta



c) Indicador 3: Índice de disponibilidad de servicio