ISSN: 2665-0398

SEGURIDAD DE LOS DATOS EN LAS EMPRESAS DE TELECOMUNICACIONES PERUANAS: UNA INICIATIVA DE SENSIBILIZACIÓN A TRAVÉS DE UNA APLICACIÓN MÓVIL

DATA SECURITY IN PERUVIAN TELECOMMUNICATIONS COMPANIES: AN AWARENESS INITIATIVE THROUGH A MOBILE APPLICATION

Tipo de Publicación: Articulo Científico
Recibido: 01/02/2026
Aceptado: 02/03/2026
Publicado: 11/03/2026
Código Único AV: e671
Páginas: 1(259-282)
DOI: https://doi.org/10.5281/zenodo.18958666

Autor:
Héctor Odín Delgado Enríquez
Ingeniería de Sistemas
Maestría en Administración de Negocios – MBA
Maestría en Docencia Universitaria
https://orcid.org/0000-0002-2388-4182
E-mail: hdelgadoe@usil.edu.pe
Afiliación: Universidad San Ignacio de Loyola
País: República del Perú

Resumen

El objetivo de este estudio fue evaluar el porcentaje de eficacia de los controles de seguridad de la información de una empresa peruana de telecomunicaciones mediante la implementación de la metodología Scrum. Se logró una tasa de cumplimiento del 85 % en la implementación de los controles de seguridad, lo que indica que la empresa ha implementado un gran número de controles para garantizar la seguridad de la información. Sin embargo, también se encontraron algunas áreas de mejora. Por ejemplo, se observó que algunos controles no se supervisaban adecuadamente, lo que podía generar riesgos para la seguridad de la información. En consecuencia, se desarrolló una iniciativa de sensibilización a través de una aplicación móvil para mejorar aún más la seguridad de la información de la empresa. La metodología Scrum resultó muy útil en este proyecto, ya que permitió un enfoque iterativo e incremental que permitió la identificación temprana de los problemas y su resolución oportuna.

Palabras Clave Aplicación móvil, metodología SCRUM, seguridad de la información, concienciación, controles de seguridad.

Abstract

The objective of this study was to evaluate the percentage of effectiveness of the information security controls of a Peruvian telecommunications company through the implementation of the Scrum methodology. A compliance rate of 85% was achieved in the implementation of security controls, indicating that the company has implemented a large number of controls to ensure information security. However, some areas for improvement were also found. For example, it was observed that some controls were not being adequately monitored, which could create information security risks. Consequently, an awareness initiative was developed through a mobile application to further improve the information security of the company. The Scrum methodology was very useful in this project, since it allowed an iterative and incremental approach that allowed the early identification of problems and their resolution in a timely manner.

Keywords Mobile application, SCRUM methodology, information security, awareness, security controls.

ISSN: 2665-0398

Introducción

Actualmente, dado el gran avance de la tecnología y la facilidad de acceso a la información que proporciona Internet, la formación virtual sobre concienciación en materia de seguridad de la información y los datos (TIC) se ha incorporado en muchas empresas internacionales como medio alternativo de refuerzo y enseñanza. Hoy en día, algunas empresas buscan estrategias para mejorar sus procesos y aumentar la productividad, teniendo en cuenta las principales ventajas que son: movilidad, conectividad y funcionalidad (Muñoz & García, 2017).

A nivel nacional, la mayoría de las empresas de nuestro país no están utilizando adecuadamente el tema de la concienciación sobre la seguridad de los datos, esto se debe a su escaso conocimiento y formación hacia los empleados o solicitantes de diferentes áreas de trabajo, ya que debido a los diferentes virus como fue el caso de la pandemia de covid-19, el trabajo presencial había disminuido y todo se gestionaba de forma virtual, en consecuencia, ha aumentado el número de robos cibernéticos, suplantaciones de identidad y fraudes. Asimismo, para desarrollar una aplicación móvil, se debe detectar una necesidad en las personas, a través de un estudio, y estas se deben ejecutar en diferentes sistemas operativos móviles (Marcillo, 2017).

De hecho, dado que Internet es una herramienta que trasciende las fronteras, rompe los límites del tiempo y el espacio. Debemos ser responsables con la seguridad que nos brinda Internet, teniendo una referencia adecuada sobre la concienciación en materia de datos para garantizar que el intercambio de nuestros datos no sea vulnerable, tanto personales como empresariales, dentro del territorio peruano y, de esta manera, contar con leyes que protejan los derechos de cada uno de los usuarios de Internet (Capponi, 2018).

En este marco, los beneficios de las TIC en las empresas se hacen evidentes, ya que pueden utilizarse de forma muy útil gracias al acceso a conocimientos gratuitos sobre diversas cuestiones de concienciación y seguridad de la información, sin necesidad de interactuar en persona como ocurría anteriormente en el caso de las guías físicas.

Por esta razón, el motivo del estudio es que, en las empresas de telecomunicaciones peruanas, la mayoría de estas se encargan de ofrecer soluciones y servicios diferenciales que se adaptan a las necesidades de los clientes. Cabe destacar que estas empresas buscan priorizar a sus clientes y tienen un alto índice de aprobación no solo a nivel nacional, como podemos ver en la figura anterior, sino también a nivel internacional, por lo que es importante formar y mejorar urgentemente la responsabilidad de los activos de información, como los datos y los usuarios, que no pueden ser manipulados de manera ilegal y perjudicial para dichas empresas de telecomunicaciones.

Revista Aula Virtual, ISSN: 2665-0398; Periodicidad: Continua
Volumen: 7, Número: 14, Año: 2026 (Enero 2026 - Junio 2026)

Como resultado de las diferentes quejas constantes relacionadas con el robo de información en los últimos cinco años debido a la falta de concienciación e información sobre la seguridad de los datos de las diferentes empresas de telecomunicaciones, ha tenido que enfrentarse a los siguientes problemas:

1. El fraude, cuyo valor de pérdidas asciende a una cuota media de millones (Muñoz & García, 2017).
2. Fuga de información, antiguos empleados hacen uso de datos de la empresa en futuros trabajos (Sisti, 2019).
3. Riesgos derivados de la mala gestión que los trabajadores hacen con los usuarios de la empresa (Capponi, 2018).

Todo ello debido a la difusión de usuarios y material confidencial, ya que cada área tiene un sistema diferente y es muy difícil para los formadores llevar a cabo esta tarea de poder supervisarlos o formarlos adecuadamente en materia de concienciación sobre la seguridad de la información y los datos, y las consecuencias de su mala gestión en estas empresas de telecomunicaciones (Muñoz & García, 2017; Sisti, 2019).

Por lo tanto, el objetivo de este artículo es demostrar la viabilidad de la aplicación móvil para aumentar el porcentaje de eficacia de los controles de seguridad de la información en las empresas, cubriendo la metodología de desarrollo y los resultados del producto (Marcillo, 2017).

Asimismo, «concienciar a los trabajadores sobre el uso adecuado de la información y los datos de la empresa objeto de estudio», a través de la tecnología de la aplicación flutter para teléfonos móviles, dicha aplicación será utilizada por los trabajadores y solicitantes de empleo de las empresas de telecomunicaciones peruanas (González, 2021).

En el contexto actual de transformación digital y con un panorama de creciente complejidad, las organizaciones deben demostrar que la información es uno de los activos más importantes de un proceso de toma de decisiones y de la continuidad operacional. El uso extensivo de plataformas digitales y sistemas de información ha aumentado también la exposición a riesgos de la seguridad de los datos, o en el caso de sectores estratégicos como es el de las telecomunicaciones, observará en su operativa diaria el manejo de grandes volúmenes de información sensible.

De este modo, la dependencia de los entornos virtuales ha puesto de manifiesto la necesidad de reforzar los mecanismos de protección de la información, no solamente desde el punto de vista tecnológico, sino también desde el comportamiento de los usuarios que interactúan con los sistemas. En ciertas ocasiones, los episodios de seguridad no son consecuencia de un fallo técnico, sino que son de

ISSN: 2665-0398

prácticas inadecuadas con respecto al tratamiento de la información, esto es una prueba de que en los procesos de formación y de educación hay mucha distancia. La situación suele ser explosiva cuando los empleados carecen de herramientas accesibles que les permitan identificar los riesgos y reaccionar a tiempo frente a eventuales episodios posteriores (Sisti, 2019; Muñoz & García, 2017).

Las empresas de telecomunicaciones cumplen un papel fundamental dentro de las organizaciones, ya que son la vía a la conectividad y el acceso a la información por lo que deben tener unos estándares de seguridad bastante altos para poder defender sus datos de los clientes, así como su propia infraestructura interna. Pero, casi siempre, la política de seguridad que se implanta radica en aspectos normativos y técnicos, dejando en un segundo plano rutas estratégicas que enfatizan la cultura de la organización y la responsabilidad personal durante el uso de la información, hecho que provocará que la implantación de controles de seguridad no sea de calidad o bien sea el foco de potenciales incidentes a consecuencia de que la falta de vigilancia en los usuarios afecte a la confianza de los mismos y a la imagen ante la institución (Sisti, 2019).

Así, la incorporación de soluciones tecnológicas focalizadas al aprendizaje continuo de los individuos con los programas de concienciación en seguridad de la información se presenta como una excepcional propuesta a fin de impulsar este proceso. Las aplicaciones móviles, por las características de accesibilidad que tienen las aplicaciones, van bien a adaptarse a los diferentes tipos de ambientes laborales (su facilidad de uso y efectuar incluso el learning en la empresa), etc.

Las aplicaciones móviles promueven la difusión del contenido con carácter continuo, la evaluación del aprendizaje y estimulan la participación de los usuarios. Su uso en los ambientes de trabajo representa una oportunidad para integrar la formación en el día a día del trabajador sin afectar demasiado las rutinas operativas (Anincubator, 2020; Cáceres & Cajas, 2017).

Así, la utilización de aplicaciones móviles de concientización proporciona la oportunidad de generar información para la gestión de la organización, ya que permite documentar datos sobre el rendimiento de los usuarios, confirmar si se están produciendo situaciones críticas y valorar hasta qué punto se están empleando las estrategias de preparación. A partir de la información obtenida, se favorece la toma de decisiones basada en datos objetivos y la preparación continua de los procedimientos de seguridad, los cuales se adecuan a las necesidades de organizaciones que actúan en un entorno muy dinámico y competitivo (Hernández, 2020; Sisti, 2019).

Revista Aula Virtual, ISSN: 2665-0398; Periodicidad: Continua
Volumen: 7, Número: 14, Año: 2026 (Enero 2026 - Junio 2026)

En este contexto, el presente trabajo tiene por objeto analizar la viabilidad del uso de una aplicación móvil como herramienta de apoyo para la concientización en seguridad de la información en una empresa peruana del sector de telecomunicaciones. Adoptando un enfoque cuantitativo, el objetivo consiste en evaluar el impacto que la aplicación tenga en la gestión de la seguridad de los datos desde el punto de vista de la posibilidad de adjuntar indicadores que permiten medir de forma objetiva los cambios que genera la intervención.

Con ello, esta línea de investigación trata de generar evidencias empíricas del uso de las tecnologías móviles como complemento a las estrategias de seguridad de la información, al mismo tiempo que contribuye a fortalecer la cultura de la protección de datos en las empresas (Hernández, 2020; Sisti, 2019).

La rápida evolución de los entornos digitales ha transformado la manera en que las organizaciones gestionan la información, y ha planteado nuevos retos en lo que se refiere a la protección de los datos y la continuidad de los servicios. En este sentido, la seguridad de la información ha dejado de ser una cuestión meramente técnica y se ha convertido en un elemento estratégico que incide en la confianza de los usuarios, en el rendimiento operativo y en la sostenibilidad de las organizaciones.

Las demandas de una tecnología cada vez más compleja y amenazante, requieren una respuesta más global que tenga en cuenta la infraestructura de aplicación informática y los implicados humanos en el uso cotidiano de los sistemas de información (Sisti, 2019).

Las empresas de telecomunicaciones, debido a ser las intermediarias del flujo de información, son especialmente vulnerables a los riesgos del tratamiento de los datos. La heterogeneidad de plataformas, sistemas y usuarios que confluyen en su seno hace que el proceso de seguridad sea más complejo y que la vigilancia y el control de las prácticas relacionadas con la protección de la información sean mucho más complicados. Todo ello pone de manifiesto la necesidad de crear mecanismos que permitan estandarizar conductas y fomentar el compromiso de los trabajadores hacia un uso responsable de los datos (Muñoz & García, 2017).

En este marco, la planificación de la capacitación tradicional pone de manifiesto limitaciones importantes para responder a las exigencias que la seguridad de la información plantea en la actualidad. Normalmente, los cursos formativos presenciales poseen por característica una temporalización efímera y la incapacidad de traducir en un cambio sostenido en el comportamiento del usuario. Ante esto, las alternativas digitales de aprendizaje permanente

ISSN: 2665-0398

suponen otra forma de plantear la concienciación, ya que hacen posible su inclusión en la jornada laboral de la organización mediante la actualización constante del conocimiento y la incorporación de nuevos riesgos (Cáceres & Cajas, 2017).

El uso de aplicaciones móviles para la concienciación sería una posibilidad de poder efectuar el abordaje de la seguridad de la información en los entornos empresariales. Este tipo de herramientas permite la personalización de los contenidos, así como también la autoevaluación por parte del usuario y la participación activa, que son esenciales para consolidar una cultura organizativa de la prevención. Además de eso, su flexibilidad y escalabilidad le permite aplicarse en distintos entornos de la empresa, independientemente de las funciones o del nivel jerárquico del trabajador (Anincubator, 2020; González, 2021).

Desde la visión de la gestión, la posibilidad de utilizar soluciones móviles contribuye también a mejorar la visibilidad de los procesos asociados a la seguridad de la información, ya que facilita la recogida de información relacionada con el rendimiento de los usuarios y el cumplimiento de las prácticas establecidas, información que servirá para identificar debilidades, ajustar las estrategias de mejora de la seguridad y reforzar los sistemas de control interno, alineando los esfuerzos de concienciación al mismo tiempo que se favorece el cumplimiento de los objetivos organizacionales (Hernández, 2020; Sisti, 2019).

Por eso, desarrollar iniciativas de aplicaciones para móviles se presenta como una respuesta adecuada a los retos actuales de la seguridad de la información de las empresas de telecomunicaciones, ya que proveen al proceso de gestión no solo de más protección a los datos, sino también de sensatez y responsabilidad personal y común, a la vez que sientan las bases para una gestión más eficaz y sostenible de los activos informacionales (Sisti, 2019; González, 2021).

Marco Teórico

Aplicaciones móviles

Una aplicación móvil se define como un sistema, este se desarrolla para ayudar a los usuarios en sus tareas diarias y profesionales (Marcillo, 2017).

Flutter

Se define como un marco de desarrollo de aplicaciones móviles multiplataforma creado por Google. Es de código abierto y permite crear aplicaciones tanto para Android como para iOS (González, 2021).

Visual Studio Code

Es un editor desarrollado por Microsoft que se puede utilizar en los sistemas operativos Windows, Linux y macOS (Castillo, 2022).

Revista Aula Virtual, ISSN: 2665-0398; Periodicidad: Continua
Volumen: 7, Número: 14, Año: 2026 (Enero 2026 - Junio 2026)

Laravel

Es un marco de código abierto cuyo objetivo es ayudar a desarrollar aplicaciones web mucho más rápido. Para su desarrollo utiliza PHP como lenguaje. La arquitectura que utiliza este marco es MVC (modelo, vista y controlador), lo que hace que las aplicaciones web sean mucho más rápidas y se adapten a cualquier proyecto que se quiera realizar (Loro, 2019).

La seguridad de la información es un aspecto primordial en las organizaciones modernas, especialmente en aquellas que pertenecen al sector de telecomunicaciones, debido al elevado número de datos que manejan cotidianamente que son sensibles. La misma aspira a garantizar la confidencialidad, integridad y disponibilidad de la información, los cuales son los pilares primordiales para la protección de los activos digitales e incluso para la continuidad de las actividades de las organizaciones.

En este sentido, la seguridad de los datos no reside sólo en la implantación de respuestas tecnológicas, sino que también reside en la implantación de políticas organizacionales y en la forma de hacer las cosas de los usuarios que interactúan con los sistemas de información (Sisti, 2019).

Algunos estudios apuntan a que uno de los principales factores de vulnerabilidad de la seguridad de la información sería el componente humano, en tanto que la falta de experiencia, formación y concienciación del personal, incrementa considerablemente el riesgo de incidentes como la fuga de información, el robo de identidad o el acceso no autorizado a los sistemas (Muñoz & García, 2017). En el contexto peruano, la incapacidad de aplicar programas estructurados de concienciación en seguridad de datos, ha llevado a la circunstancia de que el nivel de fraudes y delitos informáticos ha aumentado en los últimos años (Capponi, 2018).

La efectividad de los controles de seguridad de la información depende en gran medida del grado de conocimiento y de compromiso mostrado por los usuarios. Los controles técnicos, organizativos y operativos son insuficientes, si no se les acompaña de procesos de sensibilización que refuercen una cultura organizativa de protección de la información. La capacitación continua del personal, según Castillo (2022), permite un mayor cumplimiento de las políticas de seguridad, reduciendo a la vez los tiempos de respuesta ante incidentes, haciendo que cada parte repercuta en la eficacia del sistema de la seguridad de la información en su conjunto.

Las aplicaciones móviles han emergido, en este sentido, como un medio eficaz para dar soporte a los procesos de capacitación y sensibilización en las organizaciones. Una aplicación móvil se puede conceptualizar como un sistema informático cuyo

ISSN: 2665-0398

diseño está previsto para ser ejecutado en dispositivos de formato portátil, permitiendo al usuario el acceso inmediato y flexible a contenidos formativos y evaluativos superando la limitación temporal y espacial de la formación convencional (Anincubator, 2020). Su uso en el contexto empresarial ha permitido mejorar el compromiso de los usuarios/as y fomentar su aprendizaje autónomo, siempre que se introduzcan mecanismos de evaluación y seguimiento de la progresión del aprendizaje (Cáceres & Cajas, 2017).

La implementación de soluciones a partir del uso de aplicaciones móviles en procesos de formación corporativa ha mostrado ser una alternativa eficaz para la mejora del desempeño organizacional, ya que permiten afianzar de manera permanente los conocimientos y poder la objetividad del impacto generado por las intervenciones. González (2021) indica que tecnologías multiplataforma permiten crear soluciones fácilmente implementables por una mayor cantidad de usuarios, ya que optimizan recursos y garantizan una experiencia de uso adecuada, elementos cruciales en proyectos concretos de concientización en la seguridad de la información.

Respecto del avance tecnológico, el uso de frameworks como Flutter permite la fabricación de soluciones de aplicaciones eficientes, así como evolutivas (es decir, multiplataforma), disminuyendo los tiempos de desarrollo y mantenimiento necesarios. Este aspecto cobra especial importancia en proyectos empresariales, donde la oportunidad de la implementación y la capacidad del software, son de suma importancia para su éxito (Castillo, 2022). Además, el uso de plataformas de gestión de datos como Laravel, permitirá almacenar y procesar la información generada por los usuarios, permitiendo un seguimiento detallado en los indicadores de seguridad.

En otra vertiente, las metodologías ágiles han tomado relevancia en función de la forma de desarrollo de las soluciones tecnológicas por su forma flexible y al mismo tiempo iterativa. Tienen cabida las entregas sucesivas de productos funcionales que están en mejora continua a partir de la retroalimentación constante (Bruderer, 2019). En función de este enfoque, se presenta Scrum, que es un marco de trabajo ágil dedicado a la gestión y organización de proyectos de software, que permite organizar el trabajo de forma recurrente en ciclos breves controlados a los que denomina sprints (Honduras, 2020).

Es necesario aclarar que Scrum no es una metodología de investigación científica, sino una herramienta de gestión de proyectos que está destinada a facilitar el desarrollo de la aplicación móvil que fue el medio de intervención que se emplea en la presente investigación. Su aplicación

Revista Aula Virtual, ISSN: 2665-0398; Periodicidad: Continua
Volumen: 7, Número: 14, Año: 2026 (Enero 2026 - Junio 2026)

permitió organizar las actividades del desarrollo e ir definiendo los roles, así como permitir las entregas consultivas de funcionalidades; no influyó ninguna forma en el enfoque cuantitativo ni en el diseño preexperimental de la investigación (Bruderer, 2019; De la Cruz, 2020).

Desde la óptica de la metodología, la evaluación de la seguridad de los datos ha de pedir unos indicadores que puedan medirse de forma cuantitativa y objetiva para medir el efecto de las intervenciones que se llevan a cabo. Algunas variables como el tiempo de respuesta ante incidentes, el coste de la seguridad de los datos y el rendimiento de la protección de la información, arroja resultados sobre la eficacia de las estrategias puestas en marcha (Hernández, 2020). Este tipo de variables pueden relacionarse con aquellos escenarios antes de la intervención y su posterior puesta en marcha, posibilitando la toma de decisiones basadas en datos y la mejora continua de los procesos de seguridad (Sisti, 2019).

En su caso, las teorías expuestas avalan la utilización de una aplicación móvil como instrumento concientizado de la seguridad de los datos para empresas de telecomunicaciones peruanas y, por lo tanto, requiere la implementación de un enfoque cuantitativo para poder evaluar con objetividad el impacto que produce, garantizando una clara separación entre la metodología de investigación y las aplicaciones tecnológicas empleadas en la construcción del producto (Sisti, 2019; Hernández, 2020).

El uso del marco Scrum propició la estructuración del desarrollo a través de sprints de tiempo determinado, la especificación de roles concretos y la progresiva entrega de funcionalidades, en ningún caso interfirió con el modelo cuantitativo que proclama la investigación. Así, Scrum cumplió un papel instrumental dentro del propio estudio, y la evaluación que midió el impacto de la aplicación se realizó bajo los criterios científicos que hacen al modelo cuantitativo y al diseño preexperimental adoptado en el mismo (Bruderer, 2019; Hernández, 2020).

En este estudio se utilizó la metodología Scrum para implementar controles de seguridad de la información y desarrollar la iniciativa de concienciación a través de una aplicación móvil. Scrum es una metodología ágil que se utiliza comúnmente en el desarrollo de software para centrarse en la entrega temprana y continua de un producto de alta calidad (Bruderer, 2019).

Por otra parte, la metodología Scrum sirve para relacionar eventos, roles e instrumentos, regulando las interrelaciones y relaciones entre ellos de una manera muy simple y fácil de implementar (Honduras, 2020). De esta manera se establecieron los roles de Scrum Master y Product Owner para la misma persona, mientras que los desarrolladores se encargaron de implementar los controles de

ISSN: 2665-0398

seguridad en iteraciones de dos semanas. También se siguió un enfoque Scrum de una sola persona para el desarrollo de la iniciativa de concienciación a través de la aplicación móvil. Se establecieron los roles de Scrum Master y Product Owner para la misma persona, mientras que los desarrolladores se encargaron de implementar los controles de seguridad en iteraciones de dos semanas. También se siguió un enfoque Scrum de una sola persona para el desarrollo de la iniciativa de sensibilización a través de la aplicación móvil. Las funciones de Scrum Master y Product Owner se establecieron para la misma persona, mientras que los desarrolladores se encargaron de implementar los controles de seguridad en iteraciones de dos semanas. También se siguió un enfoque Scrum de una sola persona para el desarrollo de la iniciativa de sensibilización a través de la aplicación móvil (Honduras, 2020; Anincubator, 2020).

Metodología

La presente investigación se llevó a cabo bajo el paradigma cuantitativo, teniendo en cuenta que la misma se orienta a la medición numérica y objetiva de los efectos que una intervención tecnológica tiene sobre la seguridad de los datos en una empresa del sector telecomunicaciones. Esta modalidad de investigación permitió examinar los cambios que se producían en indicadores específicos antes y después de la aplicación de la iniciativa de concientización, mediante la utilización de procedimientos estadísticos para la interpretación de los resultados (Hernández & Mendoza, 2018).

El tipo de investigación fue de carácter aplicada, en la medida en que el estudio no se limitó a la generación de conocimiento teórico, sino que se orientó a la solución de un problema práctico que fue identificado en el contexto organizacional. Aquí la problemática estuvo vinculada al bajo nivel de eficacia de los controles de seguridad de la información, contexto que motivó el desarrollo e implementación de una aplicación móvil como apoyo en la concientización de los usuarios (Hernández & Mendoza, 2018).

En lo que respecta al diseño de la investigación, este fue de tipo preexperimental, mediante la utilización de un esquema de pretest y postest aplicado a un solo grupo. Esta modalidad de diseño permitió evaluar el impacto de la intervención a partir de la comparación de los valores de los indicadores de la variable dependiente antes y después de la aplicación de la aplicación móvil. La inexistencia del grupo de control responde a las limitaciones inherentes al entorno empresarial y a la propia disponibilidad de los registros sobre los que se operó (Hernández & Mendoza, 2018).

La población de estudio estuvo constituida por los registros de seguridad de la información de una empresa peruana del sector telecomunicaciones que incluyen información relativa a la gestión de incidentes de seguridad y a los niveles de eficiencia

Revista Aula Virtual, ISSN: 2665-0398; Periodicidad: Continua
Volumen: 7, Número: 14, Año: 2026 (Enero 2026 - Junio 2026)

en la protección de datos. Los registros constituyeron la fuente en la que se sustentó la evaluación cuantitativa de la variable objeto de estudio.

La muestra estuvo compuesta por 30 registros, obtenidos dentro de un muestreo no probabilístico por conveniencia. Este tipo de muestreo fue el más elegido al tomarlo como base por sus características de accesibilidad a los datos, de disponibilidad de la información requerida y de viabilidad operativa del estudio en el entorno organizacional que fue objeto de estudio. A partir de la muestra utilizada se obtuvo información suficiente para ser analizada en los términos planteados en el análisis, y para el análisis comparativo que se recoge en el diseño preexperimental.

La técnica de recolección de datos utilizada fue la observación, dado que se trabajó directamente sobre los registros que existían en el sistema de gestión de la empresa del caso. Para ello se utilizó como técnica de recolección de datos una ficha de observación diseñada para recoger de forma sistemática los valores que corresponden con cada uno de los indicadores que fueron definidos dentro de la operacionalización de la variable (Hernández & Mendoza, 2018).

La variable dependiente del presente trabajo fue la seguridad de los datos, que fue operacionalizada siguiendo tres indicadores principales: a) Tiempo de respuesta en los incidentes, que permitió medir la rapidez con que la organización responde a los eventos de seguridad; b) Costo de la seguridad de los datos, orientado a medir el impacto que la gestión de los incidentes tiene sobre la economía; c) Eficiencia de la protección de datos, junto a la que se valoró el grado de cumplimiento de los objetivos establecidos con respecto a la seguridad de la información. Dichos indicadores fueron cuantificados a través de fórmulas predeterminadas, que permitieron ser valoradas de manera objetiva y comparable en los momentos de la aplicación del pretest y del postest.

En cuanto a la metodología de investigación, se ha considerado lo siguiente:

1. Tipo de investigación: Aplicada
2. Diseño de la investigación: Preexperimental Enfoque de la investigación: cuantitativo.
3. Población: Registros de seguridad de datos de una empresa peruana.
4. Muestra: 30 registros
5. Técnica de recopilación de datos: Observación
6. Instrumento de recopilación de datos: Ficha de observación
7. Variable dependiente: Seguridad de los datos

Tiempo de respuesta ante incidentes

IRR = IRR - IT

Donde:

IRR = Tiempo de respuesta ante incidentes

ISSN: 2665-0398

IRR = Tiempo de respuesta ante incidentes

IT = Tiempo de respuesta ante incidentes.

Coste de la seguridad de los datos

Fórmula:

CSD = CPxS * TRA

Donde:

CSD = Coste de la seguridad de los datos

CPxS = Coste de personal por segundo

TRI = Tiempo de respuesta ante incidentes

Eficiencia de la protección de datos

Fórmula:

EPD = (TO/ TRI) * 100

Donde:

EPD = Eficiencia en la protección de datos

TO = Tiempo objetivo

TRI = Tiempo de respuesta ante incidentes

Cabe señalar que Scrum no fue utilizada como metodología de investigación, sino que fue manipulada como marco de trabajo ágil para el desarrollo de la aplicación móvil, que fue el medio de intervención del estudio. Scrum fue esgrimida para la organización, planificación y ejecución para las actividades de desarrollo del software, permitiendo un enfoque iterativo e incremental para la misma (Anincubator, 2020).

Las funciones de Scrum Master y Product Owner se establecieron para la misma persona, mientras que los desarrolladores trabajaron en el desarrollo de la aplicación en iteraciones de dos semanas. Durante el proceso Scrum se celebraron reuniones diarias de Scrum, (Anincubator, 2020) reuniones de planificación de iteraciones, revisiones de iteraciones y retrospectivas de iteraciones. En las reuniones diarias de Scrum, el investigador se reunía consigo mismo para discutir los progresos y dificultades del día anterior y planificar el trabajo del día siguiente.

En las reuniones de planificación de iteraciones se proyectaba el trabajo a realizar en la siguiente iteración. En las revisiones de iteraciones, el investigador presentaba el trabajo completado en la iteración y reflexionaba sobre los progresos. En las retrospectivas de iteraciones, se reflexionaba sobre el proceso Scrum y cómo se podía mejorar para la siguiente iteración. (Bruderer, 2019). Para almacenar los datos de los usuarios se eligió Laravel, una base de datos no relacional que se seleccionó por su simplicidad de uso y su fácil integración con la aplicación móvil (Carreno, 2012).

Durante la implementación de los Sprints, se utilizaron como referencia los requisitos funcionales y no funcionales de la aplicación móvil, que se detallan a continuación:

Revista Aula Virtual, ISSN: 2665-0398; Periodicidad: Continua
Volumen: 7, Número: 14, Año: 2026 (Enero 2026 - Junio 2026)

1. *RQF1*: La aplicación permite al usuario registrarse con datos específicos de la empresa objeto de estudio.
2. *RQF2*: La aplicación permite al usuario acceder a cursos en línea relacionados con las políticas de concienciación y seguridad de la empresa.
3. *RGF3*: La aplicación permite al usuario realizar exámenes sobre cuestiones relacionadas con las políticas de concienciación y seguridad dentro de la jornada laboral.

a. *RQF4*: La aplicación informa al usuario si el inicio de sesión ha fallado.

b. *RQF5*: La aplicación permite al usuario navegar por los diferentes módulos disponibles en la aplicación.

4. *RQF6*: La aplicación permite al usuario gestionar sus actividades y tareas relacionadas con la seguridad de los datos y la información de la empresa.
5. *RQF7*: La aplicación registra el progreso y el rendimiento de cada usuario en los cursos y exámenes realizados.

Del mismo modo, se tuvieron en cuenta los siguientes requisitos no funcionales:

1. *RQNF1*: La aplicación puede ejecutarse en cualquier dispositivo móvil de bajos recursos.
2. *RQNF2*: La aplicación es fácil de usar para cualquier usuario.
3. *RQNF3*: La aplicación funciona con fluidez, sin retrasos al iniciar sesión o cargar los contenidos.

Con la información anterior, a continuación, se detalla el trabajo realizado en cada sprint hasta alcanzar el producto completo:

Durante el primer sprint, se definió el conjunto de herramientas que se utilizarían para el desarrollo y se establecieron los objetivos en función de los requisitos de la aplicación móvil. Asimismo, se crearon maquetas que sirvieron de referencia para el trabajo en los siguientes sprints (Cáceres & Cajas, 2017).

En el segundo sprint, se implementó el módulo de inicio de sesión y registro de usuarios, estableciendo la conexión con la plataforma de la empresa para la gestión de los datos de los usuarios. Durante el tercer sprint, se llevó a cabo la integración de los cursos en línea en la aplicación, lo que permitió al usuario acceder a ellos y realizar un seguimiento de su progreso.

El cuarto sprint se centró en la implementación del módulo de exámenes, para que los usuarios puedan evaluar su aprendizaje y supervisar su progreso (De la Cruz, 2020). Finalmente, en el quinto sprint se llevaron a cabo una serie de pruebas de funcionalidad para garantizar que la aplicación funcionaba sin problemas y cumplía con todos los requisitos establecidos desde el primer sprint.

ISSN: 2665-0398

Al final de cada sprint, se presentaron los resultados del trabajo realizado, cada sprint tuvo una duración media de 2 semanas, aunque algunos fueron más cortos, lo que permitió acelerar el ciclo de desarrollo y obtener un producto funcional en el menor tiempo posible (Hernández, 2020). Una vez completado el desarrollo de la aplicación móvil, se presentaron los resultados detallando lo logrado y el porcentaje de eficacia de los controles de seguridad de la información (Vázquez, 2020).

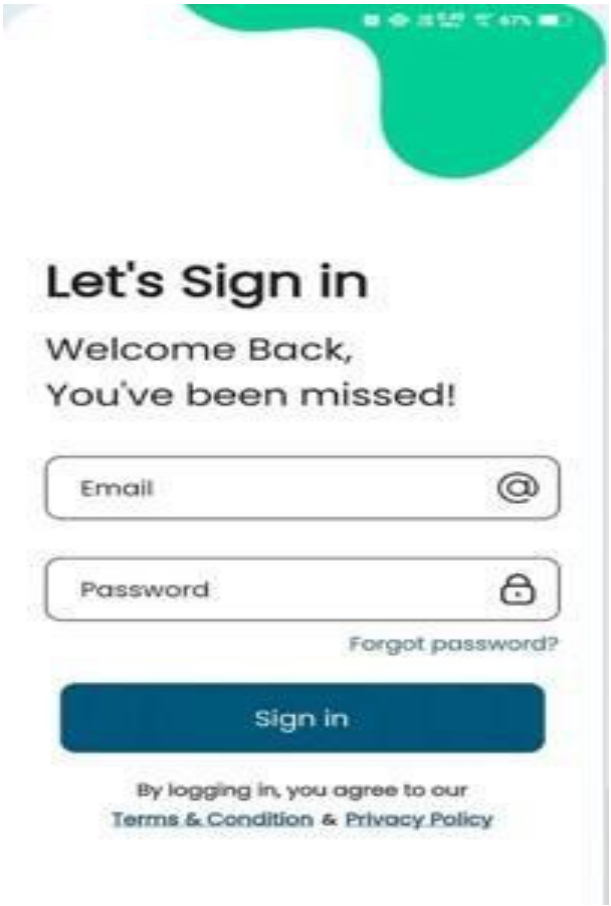

Figura 1. Módulo 1

En primer lugar, se encuentra el módulo de inicio de sesión, que se muestra en la Figura 1, en el que se presentan los campos de correo electrónico y contraseña para acceder a la aplicación a través del botón «Entrar». Además, se puede encontrar un enlace para registrarse en caso de que se trate de un nuevo usuario. La pantalla de registro se muestra en la siguiente Figura (Vázquez, 2020).

Figura 2. Módulo 2

En esta imagen se pueden ver los datos de la Figura 2 que debe introducir el nuevo usuario para poder registrarse, además de la foto que pertenecía a uno de los requisitos funcionales. Esta información se almacena en la base de datos de la plataforma Laravel para una autenticación correcta

Revista Aula Virtual, ISSN: 2665-0398; Periodicidad: Continua
Volumen: 7, Número: 14, Año: 2026 (Enero 2026 - Junio 2026)

en el momento de iniciar sesión con el correo electrónico y la contraseña definida. De esta manera, al iniciar sesión se presenta la siguiente pantalla.

Figura 3. Módulo 3

La Figura 3 muestra un grupo de módulos, detallando el nombre del usuario, los cursos y la foto que se subió en el momento del registro, de esta manera se puede navegar sin dificultad al módulo de exámenes y textos para leer que ha sido la parte principal y el objetivo de este proyecto.

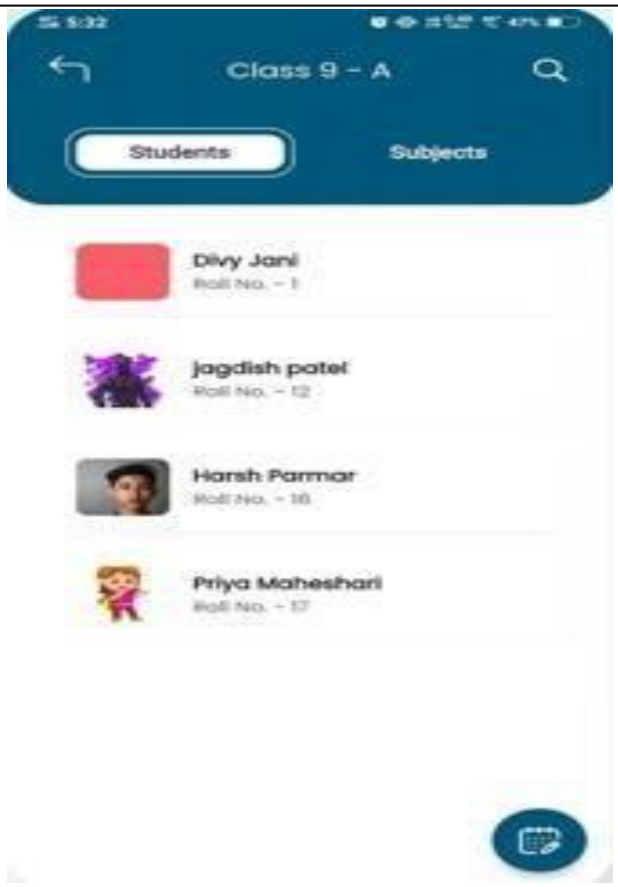

Figura 4. Módulo 4

Como se puede ver en la Figura 4, la aplicación muestra una lista de los exámenes disponibles. Tal y como se menciona en la sección de metodología, estos exámenes se almacenan en la plataforma Laravel para que la aplicación pueda abrirlos fácilmente. También hay un registro del número de pruebas realizadas por los usuarios. Este registro también se almacenará en Laravel para llevar un control de todos los usuarios registrados en la aplicación, como se muestra en la siguiente Figura.

ISSN: 2665-0398

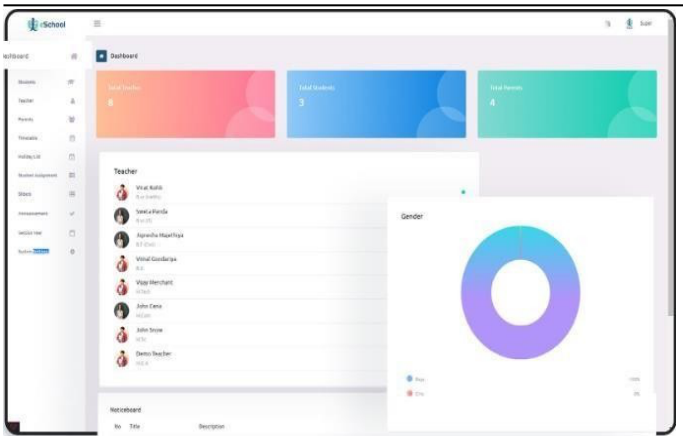

Figura 5. Módulo 5

En la Figura 5, que pertenece al panel de administración, se pueden encontrar campos que indican diferentes identificadores para cada usuario registrado. Al mostrar este identificador, se muestra el campo de exámenes realizados, como se ha mencionado, y cómo va el progreso de cada usuario, obteniendo así una forma de seguimiento.

Tras el desarrollo e implementación de la app móvil se puede resolver el problema del bajo porcentaje de eficacia de las empresas de telecomunicaciones por parte de los usuarios, utilizando esta herramienta que les proporciona exámenes y diferentes cursos para concienciar sobre la seguridad de los datos en estas empresas en el ámbito peruano.

Código para crear los indicadores en el sistema, tal y como se muestra en la Figura 6.

```
// Function to calculate the Incident Response Time (TRI)
1 usage
public static long calculateIncidentResponseTime(long finalTime, long initialTime) {
    // TRI = TF - TI
    return finalTime - initialTime;
}

// Function to calculate the Data Security Cost (CSD)
1 usage
public static double calculateDataSecurityCost(double personnelCostPerSecond, long incidentResponseTime) {
    // CSD = CPxS * TRI
    return personnelCostPerSecond * incidentResponseTime;
}

// Function to calculate the Data Protection Efficiency (EPD)
1 usage
public static double calculateDataProtectionEfficiency(long targetTime, long incidentResponseTime) {
    // EPD = (TO / TRI) * 100
    return ((double) targetTime / incidentResponseTime) * 100;
}
```

Figura 6. Código para crear indicadores en el sistema

Resultados

A continuación, se presentan los resultados descriptivos de cada indicador de la variable dependiente «Seguridad de los datos», tal y como se muestra en las Figuras 7, 8 y 9.

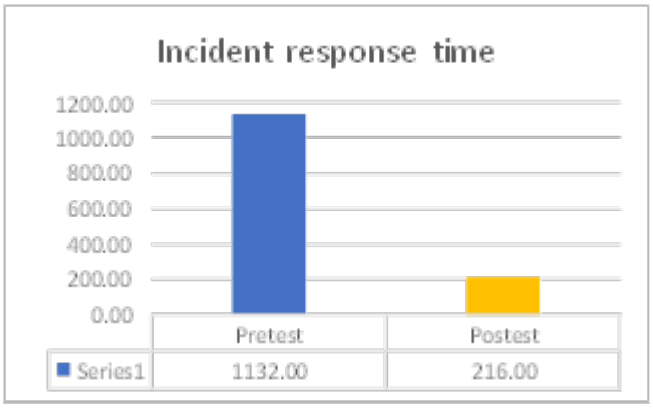

Figura 7. Descriptivos del primer indicador

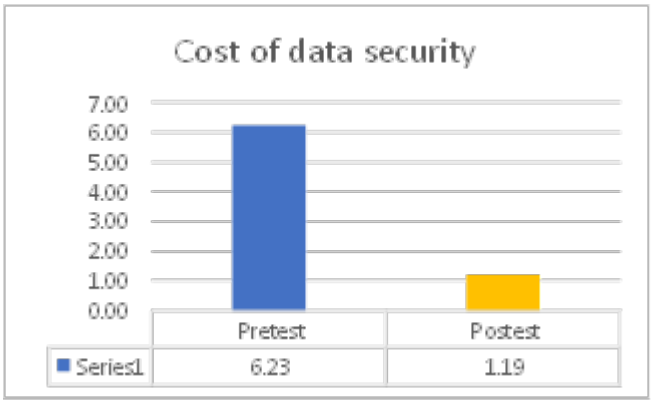

Figura 8. Descriptivos del segundo indicador

Revista Aula Virtual, ISSN: 2665-0398; Periodicidad: Continua
Volumen: 7, Número: 14, Año: 2026 (Enero 2026 - Junio 2026)

ISSN: 2665-0398

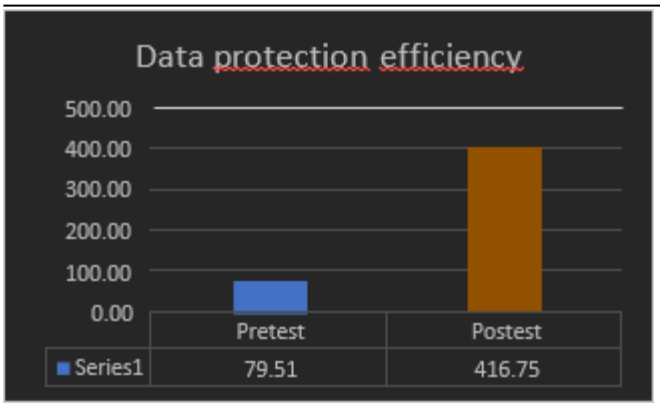

Figura 9. Descriptivos del tercer indicador

Los resultados de la prueba de normalidad de cada indicador de la variable dependiente «Seguridad de los datos» se presentan a continuación, tal y como se muestra en las Figuras 10, 11 y 12.

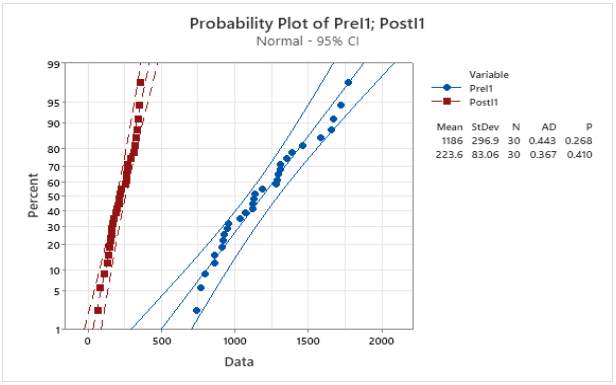

Figura 10. Prueba de normalidad del primer indicador

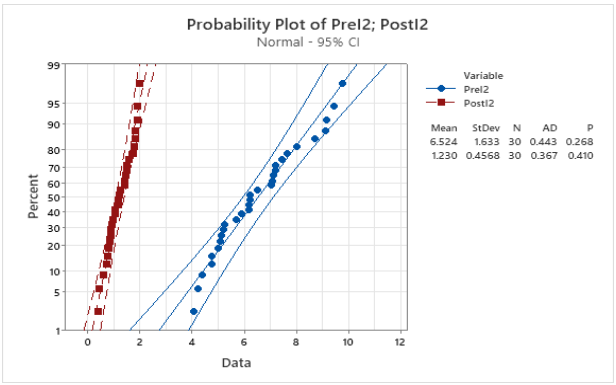

Figura 11. Prueba de normalidad del segundo indicador

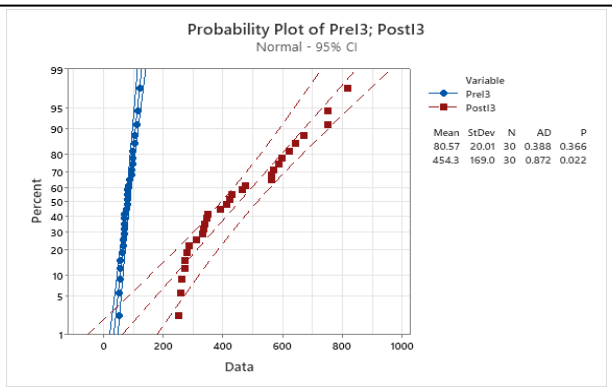

Figura 12. Prueba de normalidad del tercer indicador

Los resultados de la prueba t de Student para cada indicador de la variable dependiente «Seguridad de los datos» se presentan a continuación, tal y como se muestra en las Figuras 13, 14 y 15.

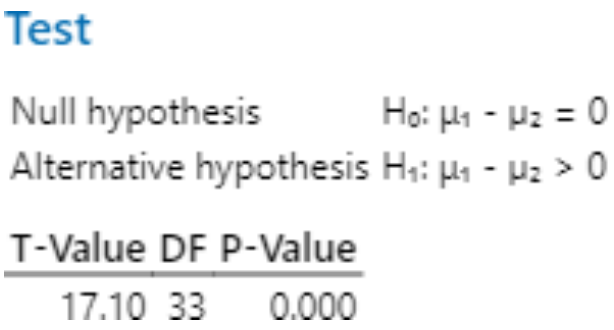

Figura 13. Prueba t de Student del primer indicador

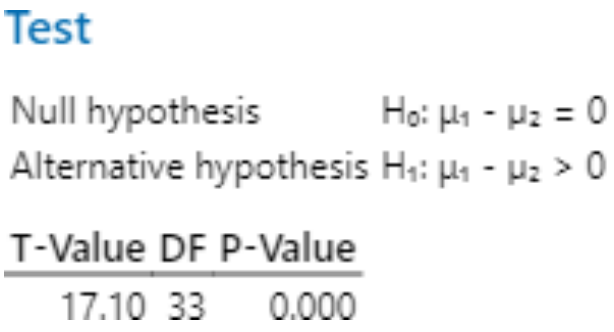

Figura 14. Prueba t de Student del segundo indicador

ISSN: 2665-0398

Test

Null hypothesis $H_0: \mu_1 - \mu_2 = 0$
Alternative hypothesis $H_1: \mu_1 - \mu_2 < 0$

T-Value	DF	P-Value
-12.03	29	0.000

Figura 15. Prueba t de Student del tercer indicador

Discusión

Los resultados obtenidos en el estudio sobre la seguridad de los datos en las empresas de telecomunicaciones peruanas, concretamente a través de una iniciativa de sensibilización sobre las aplicaciones móviles, reflejan mejoras significativas en los indicadores clave de rendimiento. El primer indicador, que mide el tiempo de respuesta ante incidentes, muestra una reducción considerable entre la prueba previa y la prueba posterior.

Mientras que en la prueba previa el tiempo de respuesta fue de 1132,00 segundos, en la prueba posterior se redujo a 216,00 segundos. Esta disminución sugiere que la implementación de la aplicación móvil ha tenido un impacto positivo en la capacidad de las empresas para responder rápidamente a los incidentes de seguridad, lo que puede atribuirse a una mayor concienciación y eficiencia en la gestión de incidentes.

En cuanto al segundo indicador, que evalúa el coste de la seguridad de los datos, los resultados también muestran una mejora considerable. En la prueba previa, el coste de la seguridad era de 6,23 unidades, mientras que en la prueba posterior se redujo a 1,19 unidades. Esta disminución del coste podría ser el resultado de una mayor eficiencia en los procesos de seguridad de los datos, quizás debido a la automatización de ciertas tareas y al aumento de la formación y preparación del personal, lo que reduce la necesidad de recursos adicionales.

Por último, el tercer indicador, que mide la eficiencia de la protección de datos, muestra una variación más compleja. En la prueba previa, la eficiencia era de 79,51, mientras que en la prueba posterior aumentó a 416,75. Este aumento podría reflejar una mejora significativa en la protección de datos, lo que es una señal positiva de que la iniciativa de sensibilización a través de la aplicación móvil ha logrado concienciar eficazmente a los empleados y usuarios sobre la importancia de proteger los datos. La aplicación no solo mejoró la velocidad y la reducción de costes, sino que también contribuyó a una mayor eficiencia en la implementación de prácticas de seguridad de datos.

Desde la modalidad metodológica, pues, los resultados alcanzados avalan la adecuación del modelo cuantitativo y del diseño preexperimental adoptado en el estudio, ya que la variación de los indicadores alcanzados permite dar cuenta de la existencia de una relación directa entre la intervención aplicada y la mejora del desempeño en seguridad de los datos. La variabilidad entre los momentos de medida anterior y posterior a la

Revista Aula Virtual, ISSN: 2665-0398; Periodicidad: Continua
Volumen: 7, Número: 14, Año: 2026 (Enero 2026 - Junio 2026)

aplicación indica que la aplicación móvil funcionó como un mecanismo acertado de apoyo de los procesos de sensibilización, validando, así, el uso de herramientas tecnológicas como mecanismos de intervención en el ámbito organizacional.

A la vez, los resultados permiten concluir que la sensibilización continua, cuando se sostiene a través de plataformas digitales, facilita la internalización de buenas prácticas en los usuarios. Esto indica que la seguridad de la información debe considerarse no solo desde un punto de vista técnico, sino también desde una dimensión educativa y preventiva. Lo anterior quiere decir, el ser humano juega un papel decisivo en lo que se refiere a la disminución de los riesgos. En lo que va en la parte que toca a la aplicación móvil, esta se comportó como un canal permanente de refuerzo, propiciando la consolidación de hábitos más responsables en lo que concierne al manejo de la información.

Una tercera cuestión digna de mención que se desprende de la discusión es la sostenibilidad de la intervención. En efecto, la utilización de la aplicación móvil, a diferencia de las sesiones de formación cara a cara no conectadas entre sí, permite ir actualizando los contenidos, así como a ir evaluando el aprendizaje en forma periódica. Todo ello, incrementa la posibilidad de mantener en la duración de los comportamientos alcanzados. Esta cuestión tiene su relevancia en empresas de telecomunicaciones donde los riesgos asociados a la seguridad de los datos están en constante evolución y requieren respuestas rápidas y actualizadas.

Además, los resultados apuntan a que la incorporación de tecnologías móviles en el tratamiento de la seguridad de la información puede contribuir a incorporar mayor capacidad sobre la toma de decisiones por parte de la organización. La sistematización de datos e indicadores cuantificables permite un seguimiento del comportamiento y, por otro lado, puede dar lugar a identificar aquellos aspectos críticos que requerirán ajustes o intervenciones complementarias. En consecuencia, la aplicación no solo orientará, sino que también jugará un papel estratégico en el propio sistema de gestión de la seguridad.

Finalmente, desde una perspectiva de la organización, los resultados del estudio muestran que la inversión en iniciativas de concientización tecnológica puede redundar en beneficios concretos (en términos de operaciones y beneficios), mejorar los procedimientos relacionados con la seguridad de los datos, aumentar la confianza organizativa interna y externa, disminuir la exposición a situaciones críticas y contribuir al cumplimiento de estándares/normas de seguridad de la información; conclusiones que abogan por la inclusión de soluciones que busquen la concientización como un eje de la seguridad de la información en el sector de las telecomunicaciones.

ISSN: 2665-0398

Conclusiones

En conclusión, la implementación de una iniciativa de concientización a través de una aplicación móvil resultó una estrategia eficaz para mejorar aún más la seguridad de la información de la empresa peruana de telecomunicaciones. La aplicación móvil proporcionó a los usuarios información relevante y de fácil acceso, las mejores prácticas para prevenir y detectar incidentes de seguridad, y los procedimientos para reportar y responder a estos incidentes. Se recomienda la implementación de iniciativas de concientización similares en otras empresas de telecomunicaciones para mejorar la seguridad de la información.

La información obtenida del estudio permite defender que la introducción de la utilización de herramientas digitales de forma sistemática orientadas a la concientización culmina como un elemento básico en el fortalecimiento de la gestión de seguridad de la información en las organizaciones dedicadas a las telecomunicaciones. Los hallazgos obtenidos hacen evidenciar que la intervención aplicada impactó positivamente en el desempeño de los procesos vinculados con la seguridad de la información obteniendo también sus evidencias a través de la mejora de la formación continua impulsada por las tecnologías móviles capaces obtener cambios medibles en el comportamiento organizacional.

De igual manera, señala la importancia de considerar la seguridad de la información no solo desde una perspectiva técnica sino como un proceso en el que intervienen las personas, los procedimientos y los sistemas. La puesta en marcha de la iniciativa permitió unir todos estos aspectos, logrando una sincronía más fluida entre las estrategias de seguridad y las operaciones de los usuarios, lo que determinó un descenso de la exposición al manejo indebido de la información.

Por la otra parte, los resultados permiten exponer de manera clara que se hace posible la evaluación en términos de los indicadores cuantitativos. Las mediciones estables sobre las variables han permitido evidenciar mejoras notables con el manejo de incidentes e incluso con la operativa, con lo que refuerza su adecuación en estudios orientados a la evaluación de la intervención en tecnologías en orden a los aspectos empresariales.

El resultado del estudio pone de manifiesto que las aplicaciones móviles son una alternativa viable y escalable para apoyar el proceso de concienciación de la seguridad de la información en aquellas organizaciones que gestionan grandes volúmenes de datos sensibles. La implementación de estas aplicaciones podrá contribuir en la mejora de la seguridad de la información mediante el fomento de una cultura organizacional orientada hacia la prevención y el buen hacer en el uso de la

Revista Aula Virtual, ISSN: 2665-0398; Periodicidad: Continua
Volumen: 7, Número: 14, Año: 2026 (Enero 2026 - Junio 2026)

información, asumiendo sólidos cimientos para futuras iniciativas relacionadas con la mejora continua del sector de telecomunicaciones.

Referencias

Anincubator. (2020). What is a mobile application? Anincubator Website. Documento en línea. Disponible https://anincubator.com/que-is-a-mobile-application/

Bruderer Vega, RS (2019). Design of a cybersecurity model for mobile devices in the business sector. *Academic Research Journal*, 18, 1-12. Documento en línea. Disponible http://hdl.handle.net/123456789/1269

Cáceres Franco, P., & Cajas Carbajal, KA (2017). Citizen security mobile application: TheShield App. Business project to obtain a degree in Banking and Finance Administration. University of Piura. Documento en línea. Disponible https://pirhua.udep.edu.pe/handle/11042/2482

Capponi Zerene, J. I. (2018). Design and implementation of a mobile application for the Cryptomarket platform. Universidad de Lima. Documento en línea. Disponible https://repositorio.ulima.edu.pe/handle/ulima/10010

Carreno Mendoza, PS (2012). Development of a personal security system that uses smartphones. Undergraduate thesis in Electronics and Telecommunications Engineering, Technical University Particular of shop. Documento en línea. Disponible https://dspace.utpl.edu.ec/handle/123456789/5127

Castillo Romero, R. M. (2022). Development of a web and mobile application for information security risk management. Universidad Nacional Mayor de San Marcos. Documento en línea. Disponible http://cybertesis.unmsm.edu.pe/handle/cybertesis/15863

De la Cruz Ahumada Coronado, EN (2020). Analysis of identity theft in social networks and its impact on the digital image of people [Graduate thesis, National University of Trujillo]. Institutional Repository National University of Trujillo. Documento en línea. Disponible https://dspace.unitru.edu.pe/bitstream/handle/UNITRU/10540/ahumadacoronado_eliana.pdf?

González, D. B. (2021). Flutter, Google's SDK for developing cross-platform apps with native performance. Documento en línea. Disponible https://profile.es/blog/que-es-flutter-sdk/

Hernández-Sampieri, R., & Mendoza, C. (2018). Metodología de la investigación: las rutas cuantitativa, cualitativa y mixta.

Hernández Vera, D. (2020). Cybernetic Identity and the Effects of its impersonation in Ecuador [Thesis, International University of Ecuador]. UIDE Institutional Repository. Documento en línea. Disponible http://repositorio.uide.edu.ec/bitstream/37000/4622/1/T-UIDE-0161.pdf

Honduras, E. (2020). Microsoft Visual Studio: Concept and applications. Documento en línea. Disponible https://www.espaciohonduras.net/

Loro Ayala, ME (2019). Proposal for the implementation of a mobile application for the occupational health and safety area of a fishing company. Undergraduate thesis in Systems Engineering, National University of Piura. Documento en línea. Disponible https://dspace.uninp.edu.pe/handle/UNI/6403

Marcillo Jaramillo, J. N. (2017). Analysis of identity theft in social networks and its influence on people's online reputation. Universidad de Guayaquil. Documento en línea. Disponible http://repositorio.ug.edu.ec/

Muñoz Díaz, K. G., & García Manrique, Á. E. (2017). Development of a mobile application for e-commerce. *Revista Tecnológica ESPOL*, 30(2), 27–37. Documento en línea. Disponible

ISSN: 2665-0398

https://doi.org/10.29019/REVTESPOCH.30.2.27-37

Sisti, MA (2019). Computer security: The protection of information in a wine company in Mendoza. *Scientific Electronic Journal of Research and Development*, 10(1), 77-88. Documento en línea. Disponible https://revistas.utp.ac.pa/index.php/REC/article/view/2064.

Vázquez Rodríguez, V. (2020). Risk factors and protection measures against identity theft in the digital sphere [Final degree project, University of Almería]. University Institutional Repository of Almeria. Documento en línea. Disponible http://repositorio.ual.es/bitstream/handle/10835/8010/TFG_VAZQUEZ%20RODRIGUEZ%2c%20VICTOR.pdf?

Revista Aula Virtual, ISSN: 2665-0398; Periodicidad: Continua
Volumen: 7, Número: 14, Año: 2026 (Enero 2026 - Junio 2026)