Recibido: 16/04/24 | **Aceptado**: 31/10/24 | **Publicado**: 16/12/24

ARTÍCULO DE INVESTIGACIÓN

Percepción del Grado de Concientización en Seguridad de Información Antes y Después de una Intervención en una Institución Religiosa en México

Perception of the Degree of Awareness in Information Security Before and After an Intervention in a Religious Institution in Mexico

Moisés Cortés Zepeda
Universidad de Montemorelos, México
0900177@alumno.um.edu.mx

Rusbel Domínguez Domínguez
Universidad de Montemorelos, México
rusbel@um.edu.mx

Omar Arodi Flores Laguna
Universidad de Montemorelos. México
oflores@um.edu.mx

Cómo citar/How to cite

Cortés Zepeda, M., Domínguez Domínguez, R., & Flores Laguna, O. A. Percepción del grado de concientización en seguridad de información antes y después de una intervención en una institución religiosa en México. *Unaciencia Revista De Estudios E Investigaciones, 17*(33), 22-38. https://doi.org/10.35997/unaciencia.v17i33.780

Resumen

El objetivo de esta investigación es: determinar si existe una diferencia significativa en el grado de concientización de la seguridad de información antes y después de una intervención en personal administrativo de una institución religiosa del centro de México. Para responder a la pregunta de investigación, ¿Existe una diferencia significativa en las medias aritméticas del grado de concientización de la seguridad de información antes y después de una intervención en personal administrativo de una institución religiosa del centro de México? se realizó una investigación de tipo preexperimental con los mismos sujetos. Para medir la concientización en seguridad de información (ISA), se aplicó el cuestionario HAIS-Q, que consta de 63 reactivos agrupados en siete áreas de interés, las cuales son: Gestión de contraseñas, uso del correo electrónico, manejo de dispositivos móviles, uso de Internet, uso de redes sociales, manejo de información y reporte de incidencias. El cuestionario se aplicó a un grupo de 26 personas de una institución religiosa del centro de México. A cada participante se le asignó un número de identificación único que solo ellos conocían. Esto se hizo con el propósito de proteger la privacidad de cada individuo y para distinguir cada instrumento, facilitando la posterior agrupación para su análisis. La aplicación del cuestionario se llevó a cabo a través de la plataforma Formularios de Google. Posteriormente, se realizó una intervención en materia de ciberseguridad combinando capacitación con historias. La intervención se enfocó en cada una de las siete áreas de interés del HAIS-Q y tuvo una duración de cinco días, con sesiones de treinta a cuarenta y cinco minutos cada una. Luego, se volvió a aplicar el cuestionario HAIS-Q al mismo grupo de 26 personas para comparar los resultados con los obtenidos en la primera aplicación. La variable de conciencia en seguridad de la información (ISA) mostró diferencias significativas en las medias ($p < .001$) y un tamaño del efecto alto ($d = 1.06$). Estos resultados confirman el rechazo de la hipótesis nula de esta investigación.

Palabras clave: capacitación, ciberseguridad, ciber amenazas, concientización, HAIS-Q, ISA.

Abstract

The objective of this research is: to determine if there is a significant difference in the degree of awareness of information security before and after an intervention in administrative personnel of a religious institution in central Mexico. To answer the research question, is there a significant difference in the degree of awareness of information security before and after an intervention among administrative personnel of a religious institution in central Mexico? A pre-experimental research was carried out with the same subjects. To measure information security awareness (ISA), the HAIS-Q questionnaire was applied, which consists of 63 items grouped into seven areas of interest, which are: Password management, use

of email, management of mobile devices, Internet use, use of social networks, information management and incident reporting. The questionnaire was administered to a group of 26 people from a religious institution in central Mexico. Each participant was assigned a unique identification number that only they knew. This was done with the purpose of protecting the privacy of each individual and to distinguish each instrument, facilitating subsequent grouping for analysis. The application of the questionnaire was carried out through the Google Forms platform. Subsequently, a cybersecurity intervention was carried out combining training with stories. The intervention focused on each of the seven areas of interest of the HAIS-Q and lasted five days, with sessions lasting thirty to forty-five minutes each. Then, the HAIS-Q questionnaire was administered again to the same group of 26 people to compare the results with those obtained in the first application. The information security awareness (ISA) variable showed significant differences in the means ($p < .001$) and a high effect size ($d = 1.06$). These results confirm the rejection of the null hypothesis of this research.

Key Words: awareness, cybersecurity, cyber threats, HAIS-Q training, ISA, training.

1. INTRODUCCIÓN

La sociedad actual es altamente dependiente de la tecnología, con la cual convive a diario. Esto conlleva la generación de millones de terabytes de datos que se transmiten a través de la red. La interacción física ha migrado hacia un espacio intangible o digital. Sin embargo, el desconocimiento de los riesgos y la falta de conciencia acerca de las amenazas a la seguridad de la información pueden poner en peligro los activos informáticos, tanto a nivel personal como institucional, y desencadenar graves consecuencias de índole económica y moral (Castañeda, 2020).

De acuerdo con el informe The Global Risks Report del Foro Económico Mundial, el aumento de las amenazas de ciberseguridad está rebasando la capacidad de la comunidad internacional para prevenirlas y gestionarlas con eficacia. El informe destaca los malware, que se incrementaron en un 358% en 2020, y los ataques de ransomware, que tuvieron un incremento muy preocupante del 435% ese mismo año (World Economic Forum, 2022).

El problema se agrava debido a la falta de profesionales en ciberseguridad. Un estudio realizado por el ISC Cybersecurity Workforce Study estima una brecha global de casi 4 millones de profesionales de la ciberseguridad para el año 2023. En México la brecha es de 116,331 especialistas en esta materia (ISC2 Cybersecurity Workforce Study, 2023).

No obstante, el mayor desafío en la seguridad de la información no radica en los elementos informáticos (hardware y software maliciosos), sino en las personas. Los expertos

coinciden en que los seres humanos representan el eslabón más débil en la cadena de protección de la información de cualquier organización (Furnell, Clarke, 2022).

Ante este panorama, los daños a la información son una realidad que conlleva graves consecuencias económicas. Existen estimaciones que calculan el coste acumulado a nivel mundial desde 2018 hasta la actualidad, derivado de los delitos cibernéticos, que asciende a unos 800 mil millones de euros (Malekos, Lostri, 2020).

De acuerdo con el informe de ciberseguridad 2021 del Centro Criptológico Nacional y Computer Emergency Response Team (CCN-CERT) de España, el 62% de los incidentes de ciberseguridad están relacionados con miembros de las organizaciones que han sido negligentes en seguridad. Esto indica que estos miembros son los causantes más comunes de este tipo de incidentes en las organizaciones, mientras que los actores internos intencionados representan el 14% de los incidentes de ciberseguridad (Centro Criptológico Nacional, Computer Emergency Response Team, 2021).

En este mismo sentido, un estudio realizado por Pricewaterhouse Coopers (PWC) señala que los empleados de las organizaciones son la causa más frecuente de violaciones de seguridad de la información (Pricewaterhouse Coopers, 2016).

Otro estudio estima que el 91% de los ciberataques se originan por errores humanos y enfatiza la importancia de la conciencia en seguridad de la información como un elemento necesario para salvaguardar a cualquier organización de las ciberamenazas. (Parsons, et al., 2017)

Adicionalmente, el CCN-CERT de España, en su informe "Ciberamenazas y Tendencias 2019", advierte sobre la necesidad de formación en ciberseguridad. Declaran que los seres humanos siguen siendo el eslabón más débil en todos los sistemas de seguridad. A pesar de que aumenta la eficacia de las protecciones en cuanto a software y hardware contra código malicioso, las medidas técnicas por sí solas no son suficientes para resolver los problemas actuales de seguridad de la información. Los ciberdelincuentes fijarán su objetivo en el ataque a las personas (CCN-CERT, 2019).

La capacitación del usuario final aborda el factor de ciberseguridad más impredecible, haciendo referencia a las personas. Si no se cumplen las buenas prácticas de seguridad, cualquier persona puede introducir accidentalmente un virus en un sistema que, de otro modo, sería seguro (Kaspersky, 2020).

La capacidad de una organización para enfrentar las ciberamenazas y vulnerabilidades está directamente relacionada con el nivel de formación y concientización de sus miembros. Es decir, a mayor formación, habrá una mayor capacidad para enfrentar las ciberamenazas y, en consecuencia, se establecerá un marco de competencias que determine qué contenidos

y niveles de formación y concientización son necesarios para cada puesto laboral (Mendevil, et al., 2022).

En la institución donde se llevó a cabo el presente estudio, se observó que existen deficiencias respecto a las buenas prácticas en seguridad de la información, como contraseñas fáciles de adivinar, la falta de uso del autenticador de doble factor, la falta de actualización de software, exposición de documentos sensibles, etc.

Las observaciones fueron basadas en los testimonios que contaban los miembros de la institución respecto a sus prácticas y lo que se percibe por parte del personal de tecnología. Varios de ellos no eran conscientes de los riesgos que conlleva la falta de buenas prácticas. De igual manera, se encontró que hay desconocimiento de los diferentes tipos de ataques que existen y el modo de operación de los ciberdelincuentes. Esto deja a los usuarios en una posición vulnerable ante los ciberataques.

Por esta razón se llevó a cabo una intervención en ciberseguridad para generar concientización, proporcionar mayor formación y mejorar las buenas prácticas en seguridad de la información.

La eficacia de este programa de intervención estará dada al dar respuesta a las siguientes preguntas:

¿Existe una diferencia significativa en el grado de concientización en la seguridad de información antes y después de una intervención en personal administrativo de una institución religiosa del centro de México?

Para comprender el objeto de estudio, a continuación, se describen las siguientes conceptualizaciones:

La seguridad informática es el área encargada de la protección lógica y física de un sistema computacional. Se establecen patrones y prácticas para minimizar los riesgos, los cuales suelen proceder del software malicioso en la misma computadora, como el malware o el spyware. Estos suelen infiltrarse en los dispositivos de los usuarios al ingresar a Internet o al insertar medios de almacenamiento extraíbles (Öğütçü, et al., 2015).

En este mismo sentido, se entiende que la seguridad de la información se basa en tres pilares: la confidencialidad, integridad y disponibilidad de la información. La confidencialidad garantiza que la información solo sea accesible para las personas autorizadas, lo que requiere controles previamente establecidos. La integridad asegura que la información se mantenga precisa y completa ante acciones o intentos malintencionados. La disponibilidad se refiere a la necesidad de que la información de un sistema esté siempre disponible para los usuarios autorizados cuando la necesiten (Domínguez, et al., 2021).

Estos pilares se ven amenazados continuamente por las fallas en los sistemas físicos y lógicos de la infraestructura de red, lo que se conoce como vulnerabilidades. La vulnerabilidad se produce cuando se viola una política de seguridad debido a la inadecuación de las reglas de seguridad o problemas en el software mismo. Estas vulnerabilidades ponen en peligro la seguridad de la información y los activos de las organizaciones (Espinoza Arana, 2018).

No obstante, las personas se consideran la vulnerabilidad más impredecible. Además, el factor humano se caracteriza por ser el más inestable y, en consecuencia, el más complicado de controlar (Universidad de Palermo. Facultad de Negocios, 2022).

Para mantener la confidencialidad, integridad y disponibilidad de la información, es importante crear conciencia sobre la seguridad de la información entre los miembros de las organizaciones, cumpliendo con los estándares adecuados de seguridad de la información y asumiendo la responsabilidad individual.

Ampliando más el concepto de concientización de la seguridad de la información (Information Security Awareness - ISA), se define como el grado en que los miembros de una organización comprenden y se comprometen con las prácticas de seguridad de la información descritas en las políticas, reglamentos y directrices de seguridad de la información de su organización. En consecuencia, actúan de acuerdo con estos lineamientos. La ISA se relaciona con el modelo de Knowledge Attitude Behavior (Conocimiento-Actitud-Comportamiento - KAB). Según el modelo KAB, se propone que, a medida que el conocimiento de un miembro aumenta los comportamientos aceptables en seguridad de la información, su actitud mejora, lo que implica un comportamiento mejor en cuanto a la seguridad de la información (Parsons, et al., enero, 2017).

En el pasado, se ha intentado medir la conciencia en seguridad de la información. En 2015, se afirmaba que la seguridad general de la información se vería significativamente afectada por la conciencia, el conocimiento y el comportamiento de un usuario de Internet. Para investigar si esta afirmación era cierta, se desarrolló el Cuestionario de Concienciación sobre la Seguridad de la Información de los Usuarios (UISAQ), que consta de una escala de 33 ítems con dos subescalas: Comportamiento Potencialmente Riesgoso y Conocimiento y Conciencia. La subescala de Comportamiento Potencialmente Riesgoso se divide aún más para centrarse en el comportamiento inusual, el mantenimiento de la computadora personal y el préstamo de datos de acceso. La subescala de Conocimiento y Conciencia se divide además en seguridad en las comunicaciones, datos protegidos y calidad de respaldo (Galba, et al., 2015).

En 2015, en Turquía, se realizó un análisis del comportamiento y la conciencia de la seguridad de la información personal. En esta investigación, se examinaron los niveles de conciencia de las personas hacia la seguridad de la información en términos de percepción y comportamiento. Los investigadores analizaron la relación que existe entre la conciencia

de los individuos hacia la seguridad de la información y sus comportamientos en el uso de las tecnologías de la información y la comunicación. Plantearon la importancia crítica de las variables que definen esta relación. El instrumento utilizado por los investigadores turcos se diseñó con el fin de proporcionar una base para una mejor toma de decisiones dentro de las organizaciones. De acuerdo con este objetivo, las escalas desarrolladas pueden ser utilizadas en el proceso de contratación y evaluación de los empleados de los sistemas de información (Öğütçü, et al., 2015).

En 2017, otros investigadores australianos utilizaron un instrumento denominado "The Human Aspect of Security Questionnaire" (HAIS-Q, Cuestionario de aspectos humanos en seguridad de información), el cual es un instrumento de medición del Índice de Conciencia de Seguridad de la Información. Está basado en el modelo de conocimiento, actitud y comportamiento (Knowledge Attitude Behavior - KAB). Estos elementos deben estar claramente especificados y relacionados entre sí. Como resultado de la investigación realizada, determinaron que el HAIS-Q aporta una contribución teórica significativa al establecer una medida válida y fiable de Information Security Awareness (ISA). Los resultados del estudio anterior y este proporcionan evidencia de la validez y confiabilidad del HAIS-Q como instrumento para medir la ISA. Además, el HAIS-Q puede predecir el comportamiento en un experimento de phishing (Parsons, et al., 2017).

En otra investigación se encontraron contribuciones teóricas y aplicadas. La principal aportación aplicada ha sido la consideración de las diferencias individuales, incluida la personalidad, en relación con la ISA (Information Security Awareness). Desde una perspectiva aplicada, esto puede ayudar a las organizaciones a identificar áreas donde pueden ser necesarias mejoras, facilitando así el desarrollo de programas de capacitación. Luego, los programas de capacitación podrían individualizarse y presentarse de manera que coincida con el perfil de personalidad y el estilo de aprendizaje de cada individuo, con el fin de maximizar los resultados del aprendizaje (McCormac, 2017).

Se ha medido la ISA en relación con varios factores. En 2020, en Australia, se exploró la relación entre la ISA, la cultura organizacional y la cultura de seguridad. Se encontró que, mientras la cultura organizacional y la cultura de seguridad estaban correlacionadas con la ISA, la cultura de seguridad desempeñó un importante papel mediador entre la cultura organizacional e ISA. Esto sugiere que las organizaciones deberían centrarse en la cultura de seguridad en lugar de la cultura organizacional para mejorar la ISA (Wiley, 2020).

Otra investigación mostró un análisis multifactorial que inhibe la implementación de un Sistema de Gestión de Seguridad de la Información (SGSI). Se encuestaron a 143 personas de dos universidades del noreste de México, en facultades de ingeniería de áreas afines. Se realizó una validación del Instrumento de Medición del Sistema de Gestión de Seguridad de la Información (IM-ISMS). Consta de 24 ítems, divididos en cuatro factores: políticas y

regulaciones organizacionales, privacidad, integridad y autenticidad. Los resultados de este estudio concuerdan con los resultados que presenta un modelo que cumple con los controles de la norma ISO/IEC 27002:2013 y los criterios de seguridad y privacidad para mejorar el SGSI. También se menciona que la implementación de controles basados en estándares ISO puede cumplir con los requisitos de las mejores prácticas de ciberseguridad. Con esta investigación se tiene el potencial de crear y validar un instrumento que mida el grado de gestión de un sistema de seguridad en la información basado en la ISO/IEC 27001 (Domínguez, et al., 2021).

En otro estudio realizado en 2022, se evaluó un sistema de gestión de seguridad de la información en una institución de educación superior en México. El propósito de este proyecto era conocer (a) el grado de conocimiento administrativo, (b) el grado de capacitación del personal, (c) el grado de compromiso de los administradores y (d) el grado de efectividad de la administración en la seguridad de la información basada en la norma ISO/IEC 27001. En este estudio, se aplicó un instrumento que incluía estas cuatro áreas de interés. Los evaluados eran empleados administrativos de la universidad y también personal del Departamento de Tecnología de la Información (DTI). Para llevar a cabo las comparaciones, se formaron tres grupos de administradores según las clasificaciones del personal administrativo. Las clasificaciones fueron las siguientes: (a) Mandos medios, (b) Gerencia media y (c) Alta gerencia. En cuanto a los resultados, los investigadores determinaron que el personal administrativo de menor rango tiene más dificultades para tomar las mejores decisiones en relación con la implementación de un SGSI (Sistema de Gestión de Seguridad de la Información). Específicamente, indicaron que los mandos medios son los que tienen un contacto directo con los alumnos y son los que menos se involucran en la toma de decisiones para la implementación de un SGSI. En este mismo sentido, se determinó que los mandos medios, al ser los ejecutores de las planificaciones de la institución, no están plenamente capacitados en los esfuerzos de la institución en seguridad de la información. Esto, a su vez, dificulta la generación de propuestas de iniciativas para la implementación de un SGSI (Sistema de Gestión de Seguridad de la Información). Esta carencia podría dar lugar a la aparición de brechas de seguridad. Los autores mencionan que la implementación de metodologías basadas en las normas ISO 27001 permite establecer un criterio sólido en los procesos de seguridad de una organización y determinar los procesos que aún faltan por implementar (Domínguez, 2022).

En otro estudio realizado en 2022 en cuatro países: Israel, Eslovenia, Polonia y Turquía se enfocaron en las relaciones entre la conciencia, el conocimiento y el comportamiento en seguridad cibernética mediante el uso de herramientas para la protección. Los resultados mostraron que los usuarios de Internet poseen una conciencia adecuada de las amenazas cibernéticas, pero aplican solo medidas de protección mínimas, que son relativamente comunes y simples. También se encontró que un mayor conocimiento cibernético está

relacionado con el nivel de concienciación, independientemente de las diferencias en el país o el género del encuestado. Además, el nivel de concienciación también está relacionado con el uso de herramientas de protección, pero no con la información que estaban dispuestos a revelar. Finalmente, se identificaron diferencias entre los países explorados que influyen en la interacción entre la conciencia, el conocimiento y los comportamientos (Zwilling, Moti, et al., 2022).

2. METODOLOGÍA

Para responder a la pregunta de investigación ¿existe una diferencia significativa en las medias aritméticas del grado de concientización de la seguridad de información antes y después de una intervención en personal administrativo de una institución religiosa del centro de México? se realizó una investigación de tipo preexperimental con los mismos sujetos.

Para medir el ISA, se aplicó el cuestionario HAIS-Q, que consta de 63 reactivos agrupados en siete áreas de interés: gestión de contraseñas, uso del correo electrónico, manejo de dispositivos móviles, uso de Internet, uso de redes sociales, manejo de información y reporte de incidencias. Cada ítem se contesta en una escala de Likert de cinco puntos, que van desde 1, 'Muy en desacuerdo', hasta 5, 'Muy de acuerdo'.

El instrumento se aplicó a un grupo de 26 personas. A cada participante se le asignó un número de identificación único que solo ellos conocían. Esto se hizo con el propósito de proteger la privacidad de cada individuo y para distinguir cada instrumento, facilitando la posterior agrupación para su análisis. La aplicación del instrumento se llevó a cabo a través de la plataforma Formularios de Google. Posteriormente, se realizó una intervención en materia de ciberseguridad, combinando capacitación con historias.

Los temas de la intervención se enfocaron en las siete áreas de interés del HAIS-Q y duró cinco días, con sesiones de treinta a cuarenta y cinco minutos cada una. La estructura de los temas expuestos fue compuesta por una descripción de las amenazas existentes, los errores que se cometen, lo que se puede hacer para prevenirse las amenazas y consecuencias y un testimonio con la experiencia de una persona conocida por los participantes respecto al tema tratado. Luego, se volvió a aplicar el HAIS-Q al mismo grupo de 26 personas para comparar los resultados con los obtenidos en la primera aplicación.

Se excluyeron los cuestionarios de ocho personas por no completar alguna de las dos pruebas: la realizada antes de la intervención o la posterior a la misma.

Análisis de datos

Para probar la hipótesis nula, se empleó la prueba estadística t de Student para muestras pareadas y Wilcoxon. Se siguieron los siguientes:

Diferencia mínima (d): se da en términos desviaciones estándar. d=

Para el tamaño del efecto de las variables que siguen una distribución normal se utilizó la d de Cohen. Los valores de referencia fueron: (a) d = .2 pequeño (b) d = .5 mediano (c) d = .8 grande (en la prueba t) (Aron, Aron, 2001).

Para el tamaño del efecto de las variables que no siguen una distribución normal se utilizó la prueba de Wilcoxon r= se aplicó el criterio propuesto por Cohen que establece la interpretación de "r" de la siguiente manera: (a) r = .1 indica un tamaño del efecto pequeño, (b) r = .3 representa un tamaño del efecto mediano y (c) r = .5 tamaño del efecto alto (Cohen, 1972).

El procesamiento de datos estadísticos se hizo con el software SPSS.

3. RESULTADOS

H_0: No existe una diferencia significativa en el grado de concientización en la seguridad de información antes y después de una intervención en personal administrativo de una institución religiosa del centro de México.

Para verificar la confiabilidad del instrumento, se llevó a cabo la prueba Omega de McDonald en los 63 ítems del HAIS-Q, aplicando esta prueba antes y después de la intervención. Los resultados se presentan en la Tabla 1, mostrando una confiabilidad bastante alta, variando desde .802 a .878 para el pretest y desde .662 a .895 para el postest.

Tabla 1.

Valores de confiabilidad Omega de McDonald.

Variable	Pretest	Postest
Gestión de contraseñas (GT)	.824	.782
Uso de correo electrónico (UI)	.836	.662
Uso del internet (UI)	.852	.872
Uso de dispositivos móviles (UD)	.839	.875
Uso de redes sociales (RS)	.802	.895
Manejo de información (MI)	.858	.815
Reporte de incidencias (RI)	.878	.819

En la tabla 2 se muestra la codificación de cada una de las variables del estudio.

Tabla 2.

Variables.

Código	Descripción
GTA	Gestión de contraseñas pretest
GTB	Gestión de contraseñas postest
UCA	Uso de correo electrónico pretest
UCB	Uso de correo electrónico postest
UIA	Uso del internet pretest
UIB	Uso del internet postest
RSA	Uso de redes sociales pretest
RSB	Uso de redes sociales postest
UDA	Uso de dispositivos móviles pretest
UDB	Uso de dispositivos móviles postest
MIA	Manejo de información pretest
MIB	Manejo de información postest
RIA	Reporte de incidencias pretest
RIB	Reporte de incidencias postest
ISAA	ISA pretest
ISAB	ISApostest

En la Tabla 3 se muestran los estadísticos descriptivos. Se observa una mayor diferencia de media en las variables ISAA-ISAB (m=20.11) y una menor en las variables RIA-RIB (m=.56).

Tabla 3.

Medias y medianas de las variables.

Variables	M1	M2	D1	Me1	Me2	D2
GTA-GTB	35.83	39.89	4.06	36.00	40.00	4.00
UCA-UCB	37.06	38.61	1.55	37.50	40.00	2.50
UIA-UIB	33.44	37.44	4.00	33.50	36.50	3.00
RSA-RSB	35.56	38.17	2.61	34.50	38.00	3.50
UDAUDB	35.94	40.94	5.00	38.00	41.50	3.50
MIA-MIB	37.89	40.22	2.33	38.50	41.00	2.50
RIA-RIB	35.00	35.56	.56	35.00	35.00	.00
ISAA-ISAB	250.7	270.83	20.11	253.00	269.00	16.0

En la Tabla 4 se presentan los resultados de los supuestos de normalidad. Se llevó a cabo la prueba de Shapiro-Wilk. Se encontró evidencia de normalidad (p > .05) en las variables UCA-UCB, RSA-RSB, RIA-RIB y en el constructo ISAA-ISAB. Estas variables fueron seleccionadas para la prueba t de Student para muestras pareadas. Las variables GTA-GTB, UIA-UIB, UDA-UDB, MIA-MIB fueron seleccionadas para la prueba de Wilcoxon.

Tabla 4.

Pruebas de supuestos de normalidad.

Variable	Estadístico Shapiro Wilk	Sig.
GTA	.941	.297
UCA	.937	.253
UIA	.966	.711
RSA	.935	.237
UDA	.875	.022
MIA	.947	.375
RIA	.968	.768
ISAA	.941	.302
GTB	.884	.031
UCB	.903	.065
UIB	.895	.047
RSB	.922	.141
UDB	.874	.021
MIB	.884	.030
RIB	.957	.551
ISAB	.948	.389

En la Tabla 5 se presentan los estadísticos para las diferencias de medias aritméticas y el tamaño del efecto, así como su interpretación.

Las variables GTA-GTB, UIA-UIB, UDA-UDB y MIA-MIB mostraron evidencia de diferencia en las medias y medianas y tamaños del efecto alto según la prueba estadística realizada, a excepción de la variable SA-RSB que mostró un tamaño del efecto mediano y las variables UCA-UCB y RIA-RIB no mostraron evidencia significativa de diferencia en las medias y el tamaño del efecto no fue significativo.

La variable de concientización en seguridad de la información (ISA) mostró diferencias significativas en las medias (p < .001) y un tamaño del efecto alto (d = 1.06). Estos resultados confirman el rechazo de la hipótesis nula de esta investigación.

Tabla 5.

Resultados estadísticos de las pruebas t de Students y Wilcoxon.

Variables	Estadístico	P	TE	Interpretación
GTA-GTB	Z=-2.446	.014	r=.58	Alto
UCA-UCB	t = -2037	.058	d= .48	No significativo
UIA-UIB	Z=-3.184	.001	r=.75	Alto
RSA-RSB	t= -2.261	.037	d= .53	Mediano
UDA-UDB	Z=3,225	.001	r=.76	Alto
MIA-MIB	Z=-2.146	.032	r= 50	Alto
RIA-RIB	t= -.916	.372	d=.21	No. significativo
ISAA-ISAB	t= -4.521	.000	d= 1.06	Alto

Z: estadístico de Wilcoxon, ***t:*** *estadístico de la prueba t muestras relacionadas* ***p:*** significación bilateral y ***TE:*** tamaño del efecto.

4. DISCUSIÓN

Se prestó especial atención en el par de variables Gestión de contraseñas (GTA-GTB), porque las contraseñas son uno de los principales objetivos de los ciberdelincuentes. Este resultado es importante, ya que se logró aumentar la conciencia en este aspecto, lo que lleva a una mejor gestión de contraseñas y un acceso más seguro a la información donde se requiere acceder y a una mayor solidez en los pilares de la seguridad de la información. El par de variables de uso del internet (UIA-UIB) presentó un resultado satisfactorio, considerando que en esta institución se emplea el internet diariamente para alcanzar los objetivos laborales y organizacionales.

El par de variables uso de dispositivos móviles (UDA-UDB) arrojó un resultado relevante. El 60% del personal está constantemente en viajes de trabajo, requiriendo el uso de múltiples dispositivos móviles fuera de las instalaciones para realizar sus labores. Esto ha logrado una proyección de menor inversión en este aspecto, ocasionada por siniestros, y ha reducido la posibilidad de daños morales.

El resultado arrojado por el par de variables uso de redes sociales (RSA-RSB) se esperaba, ya que la institución tiene un departamento dedicado a publicar contenido en redes sociales. Sin embargo, se observó un mayor impacto en el resto del personal, ya que todos utilizan alguna red social. Ahora, el personal es más consciente sobre el alcance de estas plataformas y, en consecuencia, se presta más atención a lo que se publica y a los aspectos de seguridad de sus cuentas.

Respecto al par de variables de manejo de información (MIA-MIB), se obtuvo un resultado satisfactorio debido a que la institución maneja tanto información electrónica como en formato físico. Es crucial porque proyecta una mejor gobernanza de la información. Es aún más relevante el fortalecimiento del pilar de la privacidad de información, ya que se oculta la misma a las personas que pudieran acceder sin usar contraseñas. Al mejorar la conciencia en el manejo de información, se prevendrán de manera más efectiva posibles fugas de información y los daños morales asociados.

En el par de variables uso de correo electrónico (UCA-UCB), se observó que los participantes respondieron de manera satisfactoria en el HAIS-Q pretest para esta variable (m = 37.05) y postest (m = 38.61), valores muy similares a los de otras variables en el postest. Se infiere que el personal ya tenía un grado de conciencia aceptable.

Finalmente, en el par de variables reporte de incidencias (RIA-RIB), al no observar diferencias en las medias, son similares a las medias de otras variables en el pretest. Se cree que esto se debió a la ausencia de reportes de incidencias significativas en la institución durante un período considerable, lo que hizo que este concepto fuera irrelevante para los participantes.

Los resultados muestran que la intervención en ciberseguridad influyó significativamente en la conciencia sobre la seguridad de la información de los miembros de la organización donde se realizó.

5. CONCLUSIONES

Basado en los resultados de la prueba t de students a la variable ISA, la intervención que se realizó que fue basada en capacitación intencionada combinada con historias personales fue altamente efectiva. La capacitación provee los conocimientos necesarios para un manejo más seguro de las tecnologías de información. Sin embargo, se considera que los testimonios personales tuvieron un alto impacto en la conciencia en ciberseguridad de las personas, ya que provienen de personas de confianza. Estos dos elementos combinados son fundamentales para crear entornos tecnológicos más seguros y alcanzar los objetivos organizacionales. Es crucial invertir tiempo en la producción en lugar de resolver problemas de seguridad de información.

Se tiene la satisfacción de haber contribuido a mejorar varios aspectos de la seguridad de la información. Ahora se gestionan las contraseñas de una forma más segura, siendo estas el primer guardián tecnológico de información sensible. Se navega por Internet de manera más responsable, identificando amenazas antes desconocidas. Además, se ha mejorado el cuidado en el uso de redes sociales, excelentes plataformas de comunicación

e interacción. También se presta más atención al uso de dispositivos móviles, evitando pérdidas económicas y daños morales, y reduciendo el riesgo de que la información no llegue a quien debe conocerla.

El personal de la institución puede ahora utilizar de manera más responsable y segura las tecnologías de información que les incumben.

CONFLICTO DE INTERESES

No hay conflicto de intereses de ninguno de los autores

REFERENCIAS BIBLIOGRÁFICAS

Aron, A., & Aron, E. (2001). *Estadística para Psicología*.

Castañeda, C. (2020). Concientización México y la ciberguerra. *Revista Mexicana en Ciencias Penales, 3*(10), 74–82.

CCN-CERT. (2019). *Ciberamenazas y tendencias*. https://bit.ly/31WMmr8

Centro Criptológico Nacional, Computer Emergency Response Team. (2021). *Ciberamenazas y tendencias*. https://www.ccn-cert.cni.es/informes/informes-ccn-cert-publicos/6338-ccn-cert-ia-13-21-ciberamenazas-y-tendencias-edicion-2021-1/file.html

Cohen, J. (1972). *Statistical power analysis for the behavioral sciences* (2a ed.). Lawrence Erlbaum Associates.

Domínguez, R., Flores, O. A., & Sánchez, J. A. (2021). Exploratory analysis of a measurement scale of an information security management system. *International Conference on Computer Science, Computer Engineering & Applied Computing (CSCE)*, EUA.

Domínguez, R., Flores, O., & del Valle, J. A. (2022, julio). Evaluation of an information security management system at a Mexican higher education institution. *International Conference on Computational Science and Computational Intelligence (CSCI)*, EUA.

Espinoza Arana, E. D. (2018). *Desarrollo e implementación de un sistema de control de acceso a redes inalámbricas mediante RADIUS* [Tesis de maestría, Universidad Nacional Mayor de San Marcos].

Furnell, S., & Clarke, N. (2022). Power to the people? The evolving recognition of human aspects of security. *Computers & Security, 31*, 983–988.

Galba, T., Solic, K., & Lukic, I. (2015). An information security and privacy self-assessment (ISPSA) tool for internet users. *Acta Polytechnica Hungarica, 12*(7), 149–162.

ISC2 Cybersecurity Workforce Study. (2023). *How the economy, skills gap, and artificial intelligence are challenging the global cybersecurity workforce*. https://www.isc2.org/-/media/Project/ISC2/Main/Media/documents/research/ISC2_Cybersecurity_Workforce_Study_2023.pdf

Kaspersky. (2020). *¿Qué es la ciberseguridad?* https://latam.kaspersky.com/resource-center/definitions/what-is-cyber-security

Malekos, Z., & Lostri, E. (2020). *The hidden costs of cybercrime* [Informe técnico]. McAfee. https://bit.ly/3zYkcZ1

McCormac, A., Zwaans, T., Parsons, K., Calic, D., Butavicius, M., & Pattinson, M. (2017, noviembre). Individual differences and information security awareness. *Computers in Human Behavior*. https://doi.org/10.1016/j.chb.2016.11.065

Mendevil, J., Sanz, B., & Gutierrez, M. (2022). Formación y concienciación en ciberseguridad basada en competencias: Una revisión sistemática de literatura. *Pixel-Bit. Revista de Medios y Educación, 66*, 197–225.

Öğütçü, G., Testik, Ö. M., & Chouseinoglou, O. (2015). Analysis of personal information security behavior and awareness. *Computers & Security*. http://dx.doi.org/10.1016/j.cose.2015.10.002

Parsons, K., Calic, D., Pattinson, M., Butavicius, M., McCormac, A., & Zwaans, T. (2017, enero). The Human Aspects of Information Security Questionnaire (HAIS-Q): Two further validation studies. *Computers & Security, 66*, 40–51. http://dx.doi.org/10.1016/j.cose.2017.01.004

PricewaterhouseCoopers. (2016). *Turnaround and transformation in cybersecurity: Key findings from The Global State of Information Security Survey*.

Universidad de Palermo, Facultad de Negocios. (2022). *El storytelling, el arte de contar historias con efectividad*. https://www.palermo.edu/negocios/que-es-el-storytelling.html

Wiley, A., McCormac, A., & Calic, D. (2020). More than the individual: Examining the relationship between culture and information security awareness. *Computers & Security, 88*, 101640. https://doi.org/10.1016/j.cose.2019.101640

World Economic Forum. (2022). *The global risks report*. https://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2022.pdf

Zwilling, M., et al. (2022). Cyber security awareness, knowledge, and behavior: A comparative study. *Journal of Computer Information Systems*, 82–97. https://doi.org/10.1080/08874417.2020.1712269