UNIVERSIDAD CÉSAR VALLEJO

ESCUELA DE POSGRADO

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

Gestión de la ciberseguridad y concientización digital en los usuarios administrativos de una empresa Outsourcing, Lima 2023

TESIS PARA OBTENER EL GRADO ACADÉMICO DE:

Maestro en Ingeniería de Sistemas con Mención en Tecnologías de la Información

AUTOR:

Angeles Gonzales, Edwin Ivan (orcid.org/0000-0003-2971-4616)

ASESOR:

Mg. Poletti Gaitan, Eduardo Humberto (orcid.org/0000-0002-2143-4444)

Mg. Tejada Ruiz, Roberto Juan (orcid.org/0000-0003-3669-836X)

LÍNEA DE INVESTIGACIÓN:

Auditoría de Sistemas y Seguridad de la Información

LÍNEA DE RESPONSABILIDAD SOCIAL UNIVERSITARIA:

Desarrollo económico, empleo y emprendimiento

LIMA — PERÚ

2023

Dedicatoria

Esta investigación va dedicada a mis progenitores, quienes siempre me apoyaron desde un inicio brindándome esa fortaleza y confianza para continuar estudiando y mejorando como profesional y persona.

Agradecimiento

Agradezco principalmente a Dios por permitirme avanzar en esta trayectoria, a mis progenitores Isidoro y Lucia quienes son mis verdaderos pilares, a mi hermano Cesar por el apoyo. La UCV, docentes y asesores, quienes, me ayudaron en el crecimiento profesional.

UNIVERSIDAD CÉSAR VALLEJO

ESCUELA DE POSGRADO

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

Declaratoria de Autenticidad del Asesor

Yo, POLETTI GAITAN EDUARDO HUMBERTO, docente de la ESCUELA DE POSGRADO MAESTRÍA EN INGENIERÍA DE SISTEMAS CON MENCIÓN EN TECNOLOGÍAS DE LA INFORMACIÓN de la UNIVERSIDAD CÉSAR VALLEJO SAC - LIMA NORTE, asesor de Tesis titulada: "Gestión de la ciberseguridad y concientización digital en los usuarios administrativos de una empresa Outsourcing, Lima 2023", cuyo autor es ANGELES GONZALES EDWIN IVAN, constato que la investigación tiene un índice de similitud de 12.00%, verificable en el reporte de originalidad del programa Turnitin, el cual ha sido realizado sin filtros, ni exclusiones.

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

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

LIMA, 01 de Agosto del 2023

Apellidos y Nombres del Asesor:	**Firma**
POLETTI GAITAN EDUARDO HUMBERTO **DNI:** 18073124 **ORCID:** 0000-0002-2143-4444	Firmado electrónicamente por: EPOLETTIG el 02-08-2023 14:19:55

Código documento Trilce: TRI - 0634448

INVESTIGA UCV

UNIVERSIDAD CÉSAR VALLEJO

ESCUELA DE POSGRADO

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

Declaratoria de Originalidad del Autor

Yo, ANGELES GONZALES EDWIN IVAN estudiante de la ESCUELA DE POSGRADO del programa de MAESTRÍA EN INGENIERÍA DE SISTEMAS CON MENCIÓN EN TECNOLOGÍAS DE LA INFORMACIÓN de la UNIVERSIDAD CÉSAR VALLEJO SAC - LIMA NORTE, declaro bajo juramento que todos los datos e información que acompañan la Tesis titulada: "Gestión de la ciberseguridad y concientización digital en los usuarios administrativos de una empresa Outsourcing, Lima 2023", es de mi autoría, por lo tanto, declaro que la Tesis:

1. No ha sido plagiada ni total, ni parcialmente.
2. He mencionado todas las fuentes empleadas, identificando correctamente toda cita textual o de paráfrasis proveniente de otras fuentes.
3. No ha sido publicada, ni presentada anteriormente para la obtención de otro grado académico o título profesional.
4. Los datos presentados en los resultados no han sido falseados, ni duplicados, ni copiados.

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

Nombres y Apellidos	Firma
ANGELES GONZALES EDWIN IVAN **DNI:** 46733152 **ORCID:** 0000-0003-2971-4616	Firmado electrónicamente por: EANGELESGO10 el 02-08-2023 19:50:10

Código documento Trilce: INV - 1226041

INVESTIGA UCV

Índice de contenidos

Índice de tablas

Índice de gráficos y figuras

RESUMEN

La actual investigación tomó como objetivo principal determinar la influencia de la Gestión de la ciberseguridad frente a la Concientización digital en los usuarios administrativos de una empresa Outsourcing, Lima 2023. La investigación utilizada fue de tipo aplicada con un enfoque cuantitativo y diseño no experimental, transversal correlacional. La población consistió de 250 usuarios administrativos. La muestra fue de 151 usuarios administrativos, esta fue obtenida con la herramienta Analyst STATS donde se consideró 95% del nivel de confianza y 5% de margen de error. El instrumento usado para la recopilación de los datos fue a través de un cuestionario en línea validado por el juicio de tres expertos. Respecto al análisis descriptivo se usó tablas cruzadas entre las variables y dimensiones evidenciando como resultado un nivel regular en la influencia de la Gestión de la ciberseguridad con la Concientización digital. Referente al análisis inferencial, las pruebas estadísticas demostraron una correlación alta positiva de 0.847 en Rho de Spearman y la existencia de una significancia en $p < 0.001$ entre las dos variables analizadas. En conclusión, se determinó la influencia que tiene la Gestión de la ciberseguridad en la Concientización digital en los usuarios administrativos de una empresa Outsourcing, Lima 2023.

Palabras clave: Gestión de la ciberseguridad, concientización, digital.

ABSTRACT

The current research took as its main objective to determine the influence of Cybersecurity Management versus Digital Awareness in the administrative users of an Outsourcing company, Lima 2023. The research used was of applied type with a quantitative approach and non-experimental, cross-sectional correlational design. The population consisted of 250 administrative users. The sample consisted of 151 administrative users, obtained with the Analyst STATS tool with a 95% confidence level and a 5% margin of error. The instrument used for data collection was an online questionnaire validated by the judgment of three experts. Regarding the descriptive analysis, cross tables were used between the variables and dimensions, showing as a result a regular level in the influence of cybersecurity management with digital awareness. Regarding the inferential analysis, the statistical tests showed a high positive correlation of 0.847 in Spearman's Rho and the existence of a significance at $p < 0.001$ between the two variables analyzed. In conclusion, the influence that Cybersecurity Management has on Digital Awareness in the administrative users of an Outsourcing company, Lima 2023, was determined.

Keywords: Cybersecurity management, awareness, digital.

I. INTRODUCCIÓN

En el presente, la concientización de la seguridad digital es un tema que día a día tiene mayor protagonismo y relevancia, esto debido tanto al incremento del avance tecnológico y a las amenazas cibernéticas que son cada vez más sofisticadas, por lo cual el tema de ciberseguridad es un factor necesario en el desarrollo de las organizaciones. Como se menciona en Verizon (2022) un 82% de ataques cibernéticos involucraron al factor humano por el uso indebido de los datos.

A nivel internacional, principalmente en los países desarrollados, el concepto de concientización digital viene siendo empleado a una mediana escala presentando crecimiento constante en las grandes organizaciones. Esto debido a que se detectó un factor vulnerable dentro de toda su gama de seguridad que viene a ser “el usuario” quien es un elemento necesario para la actividad de la organización. Así se menciona en un estudio realizado por Akter et al. (2022) donde afirma que la mayoría de vulnerabilidades de datos son representados en un 90% por el error humano.

A nivel nacional en Perú, el contexto de la concientización de la seguridad digital todavía continua en desarrollo, por no mencionar que solo un reducido porcentaje de las grandes empresas lo aplican en una baja medida con algunas capacitaciones esporádicas brindadas por los técnicos de tecnología de la información y no por un especialista en ciberseguridad. Por parte del estado peruano existe un procedimiento de concientización y sensibilización en la seguridad de la información que se viene aplicando en algunas entidades del estado. Como se menciona en el programa PRONABEC (2021) donde publica un plan para comunicar, sensibilizar y capacitar a los colaboradores y/o proveedores sobre el SGSI. Por parte del sector privado, algunas empresas de nivel internacional cuentan con un plan de concientización digital hacia sus usuarios que promueve el aprendizaje y cultura con el fin de optimizar sus habilidades para la identificación y prevención de los ataques cibernéticos. Según Ernst & Young (2019) indica que en el Perú solo 1 de cada 10 ejecutivos consideran que la seguridad de la información es efectiva frente a un ciberataque y 9 de cada 10 aseguran que no se dispone de presupuesto para la ciberseguridad.

En la empresa Outsourcing, este problema de falta de concientización digital es un tema que se observa a diario especialmente cuando se reciben correos electrónicos sospechosos “phishing”, los cuales en el 2023 empezaron a incrementarse en un 40% llegando a recepcionarse hasta 100 correos diariamente en las diferentes áreas de la empresa. Estas en su gran mayoría contienen enlaces web y archivos adjuntos con supuestos documentos importantes de clientes y/o proveedores; siempre con una determinada urgencia e importancia alta para una rápida respuesta. Por lo tanto, el usuario al no estar informado ni capacitado sobre puntos básicos de ciberseguridad genera automáticamente una brecha de seguridad en la empresa Outsourcing ocasionando puntos vulnerables. Hasta el momento debido a este inconveniente catalogado como el conducto principal para el ingreso de diversos ataques cibernéticos de malware (Ransomware, spyware, troyanos, virus, gusanos, etc.) la empresa Outsourcing se ha visto comprometida en más de 5 oportunidades con la perdida de información, ingresos no autorizados e intentos de desfalco financiero a las diversas cuentas bancarias. En general la problemática de esta investigación recae en la falta de concientización de los usuarios causado por el desconocimiento de las amenazas cibernéticas actuales y la falta de cultura sobre la ciberseguridad.

La relevancia de esta investigación en el aspecto social contribuye a fomentar conciencia en la ciberseguridad; en el aspecto empresarial contribuye con la protección y prevención de amenazas cibernéticas; por último, en el aspecto profesional colabora con la formación de competencias y destrezas en el campo de la ciberseguridad.

Debido a los acontecimientos informáticos descritos líneas arriba, se esbozó como problema general la siguiente interrogante ¿La gestión de la ciberseguridad influye en la concientización digital en los usuarios administrativos de una empresa Outsourcing, Lima 2023? Asimismo, se planteó los problemas específicos: ¿La evaluación de riesgos de la gestión de la ciberseguridad influye en la concientización digital en los usuarios administrativos de una empresa Outsourcing, Lima 2023?, ¿Las políticas de seguridad de la gestión de la ciberseguridad influyen en la concientización digital en los usuarios administrativos de una empresa Outsourcing, Lima 2023?, ¿La supervisión de actividades de la gestión de la

ciberseguridad influye en la concientización digital en los usuarios administrativos de una empresa Outsourcing, Lima 2023?.

Esta investigación cuenta con una justificación práctica, la cual tiene la finalidad de generar un nivel de cultura en el usuario que le permita conocer los peligros existentes y estar preparado para reconocerlos. A través de esto se busca mejorar la concientización de la seguridad digital en los usuarios administrativos demostrando los riesgos que representan los ataques cibernéticos.

En relación al objetivo general del estudio se planteó: Determinar la influencia de la gestión de la ciberseguridad en la concientización digital en los usuarios administrativos de una empresa Outsourcing, Lima 2023. También, se estableció tres objetivos específicos: Determinar la influencia de la evaluación de riesgos de la gestión de la ciberseguridad en la concientización digital en los usuarios administrativos de una empresa Outsourcing, Lima 2023. Determinar la influencia de las políticas de seguridad de la gestión de la ciberseguridad en la concientización digital en los usuarios administrativos de una empresa Outsourcing, Lima 2023. Determinar la influencia de la supervisión de actividades de la gestión de la ciberseguridad en la concientización digital en los usuarios administrativos de una empresa Outsourcing, Lima 2023.

Concerniente a la hipótesis general del estudio se señaló: La gestión de la ciberseguridad influye significativamente en la concientización digital en los usuarios administrativos de una empresa Outsourcing, Lima 2023. Asimismo, se señaló las hipótesis específicas: La evaluación de riesgos de la gestión de la ciberseguridad influye significativamente en la concientización digital en los usuarios administrativos de una empresa Outsourcing, Lima 2023. Las políticas de seguridad de la gestión de la ciberseguridad influyen significativamente en la concientización digital en los usuarios administrativos de una empresa Outsourcing, Lima 2023. La supervisión de actividades de la gestión de la ciberseguridad influye significativamente en la concientización digital en los usuarios administrativos de una empresa Outsourcing, Lima 2023.

II. MARCO TEÓRICO

En esta investigación se utilizaron artículos de revistas indexadas correspondientes a los temas de Gestión de la ciberseguridad y concientización digital, así mismo de estudios que abarcan las dimensiones indicadas.

Como antecedente internacional se consideró a Nwankpa y Datta (2023) con el estudio que se enfoca en los roles de la conciencia cibernética y políticas de seguridad realizado en los EE. UU, cuyo objetivo fue explorar cómo el trabajo remoto influye respecto a la conciencia de seguridad cibernética de los empleados y a la toma de precauciones en la seguridad. La metodología utilizada fue la investigación exploratoria con un enfoque cuantitativo mediante encuesta. Su muestra empleó a 203 trabajadores remotos de múltiples organizaciones. Los resultados mostraron que el trabajo remoto en un 38% fue considerado como un factor desencadenante clave para concienciación sobre ciberseguridad, lo cual afecta positivamente de forma directa e indirecta en la seguridad. La conclusión fue que la capacitación, educación y gobernanza sobre la conciencia en ciberseguridad influye de forma positiva manifestando comportamientos autorregulados en los usuarios.

Además, Boto-Garcia (2023) en su estudio sobre la concienciación y formación del personal frente a los ciberataques y riesgos digitales en España, consideró como objetivo estudiar la relación de la concienciación y la formación de los empleados de una hostelería respecto a los temas de ciberdelincuencia y ciberataques en una entidad. La metodología empleada fue exploratoria de tipo transversal basada en encuestas. La muestra fue representativa tomada de Pymes de hostelería de un total de 677 pertenecientes exclusivamente al grupo NACE. Como resultado del análisis detectaron que los ataques cibernéticos sufridos sin una preparación previa son significativamente mayores frente a una situación donde los empleados cuentan con una preparación previa, mostrando así una diferencia de 0.353 y 0,468 en algunos casos. En conclusión, se determinó que las capacitaciones brindadas por las Pymes sobre ciberseguridad no están siendo efectivas, debido a que la diferencia detectada entre el personal capacitado y sin

capacitar es mínima dejando de esta manera algunas brechas de seguridad que afectan a la empresa.

Además, Fadlika et al. (2023) en su estudio sobre la concientización en la seguridad de la información a los usuarios del sector de energía realizado en Indonesia, sostuvo como objetivo calcular el grado de concientización de la seguridad de la información, con ello investigar la correlación entre el conocimiento, actitud y conducta del personal de la empresa. La metodología utilizada fue cuantitativa empleando como instrumento el cuestionario. La muestra fue de 130 participantes del sector de energía de la empresa PT ABC. Los resultados mostrados fueron de 0.919 de confiabilidad y 0.108 en la correlación de Pearson; la evaluación de hipótesis empleó un método de regresión para la obtención de una significancia entre las dimensiones en el modelado de Conocimiento, Actitud y Comportamiento (KAB). Las conclusiones demostraron la existencia de una alta conciencia en la seguridad de la información, mientras que, en otros aspectos como el uso de internet, manejo de información y gestión de activos requieren mejorar la concientización.

De forma similar, Khan et al. (2023) en el estudio sobre la evaluación de la motivación de protección apoyada en la capacitación de concientización sobre seguridad cibernética empleando el modelo Kirkpatrick realizado en Pakistán, tuvo como objetivo comprender el comportamiento después de la implementación del entrenamiento en ciberseguridad. La metodología empleó una investigación cuasi experimental pre-post. La muestra fue de 154 estudiantes universitarios de informática y artes digitales. Los resultados obtenidos fueron que la capacitación basada en PMT a los estudiantes permitió aumentar el conocimiento de las amenazas cibernéticas y aplicar estrategias para contrarrestarlas. En el componente PMT se identificó que la autoeficacia es significativa en el comportamiento en ciberseguridad. La conclusión fue que la capacitación en ciberseguridad incrementó significativamente la autoeficacia de los estudiantes y contribuyó con la concientización en ciberseguridad.

Asimismo, Reeves et al. (2023) realizo un estudio sobre las percepciones de los empleados sobre la seguridad cibernética, cuyo objetivo fue abordar la brecha de percepción y respuestas de los empleados frente a la observación de videos de ciberseguridad. La metodología que utilizó fue una investigación cualitativa con

entrevistas semiestructuradas. La muestra en el primer estudio fue de 24 entrevistas al personal de diferentes industrias y en el segundo estudio a 457 adultos a los cuales se analizó las puntuaciones de Escala de Fatiga de Consejos de Seguridad Cibernética (CAFS). Los resultados en ambos estudios arrojaron que los empleados hacen inferencias sobre la motivación corporativa desde una perspectiva de seguridad cibernética. Como conclusión se obtuvo que los dos estudios se ubican entre los primeros en combinar la técnica Repertory Grid de Personal Construct Psychology (PCP) para un análisis hibrido deductivo e inductivo de respuesta de los empleados sobre el programa de Educación, Capacitación y Concientización sobre Seguridad (SETA) apoyados en los resultados de CAFS para la capacitación en seguridad cibernética.

De similar manera, Hillman et al. (2023) en el estudio al respecto de la evaluación sobre la concientización del phishing en las empresas realizado en Israel, tuvo como objetivo examinar la efectividad de la capacitación en concientización del phishing organizacional. La metodología empleada fue una investigación cuantitativa donde se analizó un conjunto de campañas de phishing dirigidos a los usuarios de una organización. La muestra fue de 5000 empleados de una institución financiera. Los resultados demostraron que las tres oleadas simuladas de phishing obtuvieron en la primera oleada un 25%, segunda oleada 13% y tercera oleada 10% con una desviación estándar en promedio de 7.43%, por lo que demuestra que las actividades de concientización organizacional previas son efectivas. De esta forma respaldan la H1 donde se indica que las vulnerabilidades se reducen a través de las capacitaciones sobre phishing brindando una mejora continua. La conclusión del estudio fue que la prevención ante los ataques de phishing es la capacitación a los usuarios para mejorar la conciencia y el comportamiento proactivo teniendo en cuenta el desafío que se pueda presentar en una organización.

Adicionalmente, Krawczyk y Caputa (2023) en el estudio sobre la conciencia de la seguridad de la red y perspectiva del cliente realizado en Polonia, tuvo como objetivo evaluar la conciencia de seguridad en la red entre el cliente y empresa. La metodología usada fue una investigación cualitativa donde emplearon datos estadísticos mediante cuestionarios. La muestra utilizada fue de 1245 personas de residencia polaca entre la edad de 10 a 70 años, a quienes se les aplico un sondeo

de forma aleatoria. Los resultados logrados fueron que las empresas polacas detectaron que el avance digitalización no permite un control adecuado en la ciberseguridad y la protección de datos. La conclusión del estudio determinó que el grado de conciencia de seguridad de red de los usuarios presenta una falsa convicción debido, a que se sobreestiman las habilidades digitales de percepción, acción y conocimiento de los usuarios.

Así también, Huraj et al. (2023) en el estudio sobre Medición de la conciencia de seguridad cibernética entre estudiantes de computación y ciencia de medios realizado en Eslovaquia, tuvo como objetivo examinar las actitudes y conciencia de los estudiantes universitarios sobre la ciberseguridad. La metodología usada fue no experimental, cuantitativa y descriptiva. La muestra usada constó de 570 estudiantes de Ciencias de la Computación y Ciencias de medios. Los resultados referentes al análisis estadístico fueron casi similares entre ambas ciencias. Respecto a la importancia de la ciberseguridad los estudiantes de Ciencia de Computación la consideran importe un 70.70% y los estudiantes de Ciencia de medios un 69.92%. La conclusión fue que los estudiantes de la Ciencia de Computación y los estudiantes de la Ciencia de Medios presentan casi una misma actitud de conciencia frente a los problemas de ciberseguridad dando una ligera diferencia con los que tienen formación en informática.

También, Tejay y Mohammed (2023) en el estudio orientado a una cultura de seguridad para el éxito sobre la seguridad de la información apoyado en una perspectiva antropológica realizado en USA, tuvo como objetivo comprender la importancia de la seguridad de la información y el impacto del éxito que genera en una organización. La metodología usada fue una investigación mixta empleando entrevistas semiestructuradas y encuestas. La muestra fue de 25 entrevistas a profesionales de ciberseguridad y 473 encuestas realizadas a usuarios en línea de varias organizaciones. Los resultados fueron que la implementación de la Cultura de la Seguridad de la Información obtuvo 59.8% (R^2 = 0.598) y la variable de Percepción del éxito en Seguridad de la Información fue 24.3% (R^2 = 0.243). Obtuvo una significancia de 0.128, p= 0.006 reforzando lo planteado en la H1, así mismo H2, H3, H6 y H7 tuvieron una significancia excepto H4 y H5, los cuales no obtuvieron resultados significativos. La conclusión del estudio fue que existe una cohesión entre el código profesional, la conciencia de la seguridad de la información

y las experiencias laborales informales, los cuales influyen sobre la cultura de seguridad de la información en una entidad.

De forma similar, Rawindaran et al. (2022) en el estudio respecto al impacto de la concienciación de ciberseguridad en las PYMES usando software inteligente para combatir el ciberdelito realizado en Gales, tuvo como objetivo explorar cómo las PYMES están controlando el ciberdelito, administrando sus actividades en línea y concientizando al personal sobre ciberseguridad para una prevención de amenazas cibernéticas. La metodología usada fue una investigación cuantitativa empleando cuestionarios. La muestra fue de 122 colaboradores de PYMES galesas. Los resultados demostraron la existencia de grandes brechas en la toma de conciencia y desconocimiento del uso de software de seguridad cibernética donde se reflejó que solo un 30% entendía la terminología. La conclusión del estudio fue que las estrategias de Exploración del impacto de la Concientización sobre Ciberseguridad en Pequeñas y Medianas Empresas (SME) ayudan a comprender los riesgos y planificar contingencias para mantener los datos seguros y protegidos frente amenazas cibernéticas.

También, Mendivil et al. (2022) en el estudio sobre la concienciación cibernética frente amenazas y vulnerabilidades realizado en España, tuvo como objetivo estudiar el uso de modelos de aptitudes en programas de instrucción y concientización en ciberseguridad enfocados a los usuarios no TIC de una organización. La metodología usada fue cualitativa compuesta por registros de base de datos de revistas. La muestra fue de 1300 artículos, los cuales pasaron por tres fases; la primera fase 1300 artículos, en la segunda fase 49 artículos y la tercera fase 10 artículos. El resultado fue la comprobación de un alto número de artículos sobre la formación y la concienciación de la ciberseguridad, pero el nivel de competencia mostrado es bajo, ya que solo se enfoca en tres aspectos: patrones de seguridad, análisis interno y juicio de expertos, lo que conlleva limitaciones. La conclusión fue que el grado de aptitudes en las acciones de instrucción y concienciación de la ciberseguridad aplicada en los usuarios no TIC de una organización son muy escasos, además que las metodologías empleadas al parecer son suficientes, pues no parecen ser revisadas ni actualizadas.

Asimismo, Akter et al. (2022) en el estudio sobre la competencia de concienciación sobre la ciberseguridad en una economía digital realizada en

Australia, cuyo objetivo fue identificar las dimensiones de las capacidades de concienciación sobre la ciberseguridad en una organización en una economía digital basada en datos. La metodología que empleó fue una investigación exploratoria con una revisión metódica de la literatura (SLR). La muestra tomada fue de 62 artículos vinculados con la concienciación de la ciberseguridad. Los resultados del estudio demostraron que el comportamiento de los usuarios puede variar por medio de la educación, sobre todo frente a una amenaza de seguridad; considerando necesariamente la capacitación y entrenamiento con ejemplos reales. Su conclusión fue que el desarrollo de la Concientización sobre las Capacidades de Ciberseguridad (CSAC) puede ser empleada en diversas organizaciones específicas, pero que cuenten con la interacción y compromiso de los usuarios finales.

También, Datt y Tewari (2021) en el estudio sobre la actitud y conciencia de los usuarios hacia la seguridad cibernética realizado en la India, tuvieron como objetivo analizar las actitudes y conciencia de los usuarios frente a la ciberseguridad clasificados por el género, estado laboral y calificaciones. La metodología del estudio fue cuantitativa empleando un cuestionario. La muestra se realizó a mujeres y hombres de una empresa, quienes manipulan un equipo informático para laborar. Los resultados fueron que el 34% de mujeres y el 28% de hombres desconocen los riesgos de intercambio de información personal en internet. El 51% de mujeres y el 38% de hombres desconocen los problemas básicos de seguridad, ataques de phishing, ingeniería social y riesgos al utilizar el Wifi público. Como conclusión determinaron que más del 85% del personal cuenta con habilidades en TI. Dichas habilidades se miden con los siguientes criterios: fundamentos de TI, aplicaciones básicas de oficina y habilidades de internet, pero un escaso nivel de concientización de la seguridad cibernética.

En congruencia con los antecedentes locales se tiene a Santisteban et al. (2020) en el estudio sobre el análisis de las estrategias nacionales de ciberseguridad, cuyo objetivo fue analizar y diseñar Estrategias Nacionales de Ciberseguridad para mitigar ataques cibernéticos. La metodología empleada fue una investigación exploratoria y descriptiva enfocada en las estrategias de ciberseguridad nacional. La muestra fue tomada de 20 países europeos que han

implementado el desarrollo de estrategias y políticas de seguridad. El resultado se obtuvo tras un análisis de las estrategias de los diferentes ataques clasificados por países donde Rusia obtuvo un 42%, Brasil 21% y Alemania 15%, siendo así los países más afectados por los ciberataques. La conclusión fue que tras el análisis de las estrategias de ciberseguridad determinaron aplicar las estrategias para combatir el cibercrimen y con ello poder ayudar a los usuarios a sensibilizarse para prevenir los ciberataques.

Además, Ormachea (2020) en su estudio sobre las estrategias de ciberseguridad para el reforzamiento de la seguridad, tuvo como propósito proponer tácticas integrales de ciberseguridad para el reforzamiento de la seguridad local del Perú. La metodología usada fue no experimental con forma descriptiva y enfoque epistemológico. La muestra empleada fue compuesta por estrategias de ciberseguridad aplicadas en los Países bajos, USA, España y Perú. Los resultados obtenidos fueron que el estado peruano aún continúa en desarrollo con los enfoques de concientización y capacidades cibernéticas al respecto. En conclusión, determinó que la ciberseguridad es un compromiso social de la parte pública y privada, por lo que, la estrategia de Ciberseguridad del Perú es un requisito que debe ser completado.

La teoría que se relaciona con esta investigación es la teoría de Defensa en profundidad, donde Moreno (2008) tiene como premisa que ninguna disposición de seguridad es segura y que los atacantes pueden superar cualquier sistema de seguridad individual si tienen suficiente tiempo y recursos. Por lo tanto, para mitigar los riesgos, se deben implementar varias barreras de seguridad en diferentes niveles, de manera que, si una capa es comprometida existan otras capas que aún puedan prevenir o detectar los ataques. De similar manera, Rodríguez (2020) indica que la Defensa de profundidad se trata de un sistema de protección en capas que impide la filtración de amenazas tanto internas como externas para que la organización tenga una protección considerable de la información.

Adicionalmente, se considera la teoría del comportamiento planificado (TPB) debido a que se orienta al enfoque de concientización. Como lo indica Seyal et al. (2017) indican provenir desde un principio base para determinar las actitudes, los elementos subjetivos y el control percibido que conducen a las tentativas del

comportamiento. También, Ajzen (1991) señala que la teoría del comportamiento planificado contempla a la conciencia, planificación y razonamiento de un individuo donde la intención y control son los puntos clave.

En relación a la conceptualización de la variable independiente Gestión de la ciberseguridad, la Resolución peruana SBS N° 504-2021 (2021) menciona a la gestión de la seguridad de la información y ciberseguridad (SGSI-C) como una lista de reglas, procedimientos, técnicas, funciones y actividades diseñadas para identificar y resguardar los activos de información, identificar incidentes de seguridad, predecir respuestas y recuperarse de incidentes de ciberseguridad. También, la Fundación Telefónica (2016) indica sobre las fases de la gestión de la ciberseguridad donde expresa que se trata de un proceso que se compone de la prevención, detección y respuesta sin dejar de lado al aprendizaje que permite una fluidez en la mejora continua.

En correlación con las dimensiones que abarca la variable independiente Gestión de la ciberseguridad se consideró las siguientes: Evaluación de riesgos, políticas de seguridad y supervisión de actividades.

Sobre la dimensión evaluación de riesgos Pinzón (2014) señala que es un proceso de identificación, análisis y valoración donde permite establecer un grado de amenaza y riesgo asociado teniendo en consideración el resultado del proceso y la identificación de los controles adecuados. En concordancia, Główczyńska (2010) menciona que la evaluación de riesgos consiste en una serie de procesos lógicos diseñados para analizar y evaluar sistemáticamente los peligros potenciales para la seguridad o la salud. Adicionalmente, De Freitas (2009) señala que la evaluación de riesgos es un procedimiento de estimación de riesgos y criterios establecidos, teniendo la finalidad de determinar el grado de importancia en una organización que desea contemplar un Sistema de Gestión de la Seguridad de la Información.

Sobre la dimensión políticas de seguridad Gómez (2011) señala que se trata de declaraciones que cubren la seguridad de los sistemas, los cuales contienen definiciones y delimitaciones de responsabilidades técnicas y empresariales. Por su parte, Vega (2008) indica que la política de seguridad no solo se trata de conocer las amenazas expuestas y recursos, sino en instaurar un origen, las cuales pueden

ser internas o externas. También, Dussan (2006) menciona que se considera como un instrumento que permite manejar un problema o situación con la finalidad de orientar a los miembros de una organización.

Sobre la dimensión supervisión de actividades Valdivia (2014) menciona a la supervisión como un compuesto de actividades técnicas y morales que tienen la finalidad de avocarse a una mejora continua y desarrollo en una organización. Así mismo, Chiavenato (2001) define la supervisión de actividades como una función gerencial que se implementa a nivel operativo de la empresa. El supervisor es un director que dirige las actividades de un gerente no ejecutivo, es decir, una persona que no desempeña funciones administrativas en la empresa.

Respecto a la conceptualización de la variable dependiente Concientización digital. Karakuş y Kılıç (2022) indican que la conciencia digital es una capacidad de conocer, apreciar y observar el entorno que rodea al individuo en afinidad al campo de las tecnologías digitales. Asimismo, Vidal et al. (2021) indica que la conciencia digital va referenciado a una conciencia personal relacionado a las Tecnologías de la Información como la identidad en línea, huella digital y el uso en general. También, Corletti (2017) enfatiza a la sensibilización como una responsabilidad común donde los usuarios ejercen un rol primordial en la seguridad, por lo tanto, deben ser conscientes de los riesgos en línea que lleguen a presentar y saber cómo protegerse.

Referente a las dimensiones que abarca la variable independiente Concientización digital se consideró las siguientes: Conocimiento tecnológico, habilidad digital y seguridad digital.

Respecto a la dimensión conocimiento tecnológico Koehler y Mishra (2008) mencionan que el conocimiento tecnológico hace referencia a todo tipo de conocimiento tecnológico que no solo abarque temas de informática, sino que abarca otros campos de conocimiento. También, Arenas et al. (2005) mencionan que el conocimiento tecnológico es un atributo que fundamenta la actividad, por lo cual brindan una base explicativa en relación a la teoría y la práctica siempre con un acoplamiento de la información

Respecto a la dimensión habilidad digital Morduchowicz (2021) indica que se trata de un conglomerado de conocimientos, portes, artes, condiciones y destrezas que se necesitan para usar las tecnologías. Así mismo, Levano et al. (2019) lo

menciona como competencias digitales que son comprendidas bajo diversos conceptos de líneas de estudio, los cuales abarcan proyecciones de aprendizaje, investigación, recreación y relaciones sociales, enfocadas al rubro de la tecnología. Asimismo, DGTIC (2014) lo define como un compuesto de conocimientos entrelazados con el uso de los recursos de comunicación, el ingreso de la información, el procesamiento y producción.

Respecto a la dimensión seguridad digital Hernández (2022) menciona a la seguridad digital como un compuesto de acciones que sirven para proteger y controlar las comunicaciones, información y datos siempre con la premisa de la triada sobre seguridad de la información. También, Castillejos (2016) señala que la seguridad digital no solo se trata de resguardar al usuario y dispositivos, sino a una protección general, donde se incentive a tomar conciencia de las herramientas digitales y el uso de la tecnología que se utilice.

III. METODOLOGÍA

3.1 Tipo y diseño de investigación

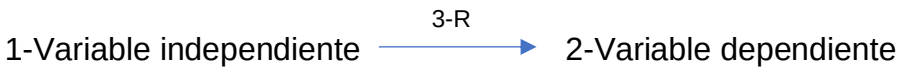
3.1.1 Tipo de investigación

En este estudio se empleó el tipo de investigación aplicada, ya que se buscó resolver un problema determinado. De acuerdo a Ñaupas et al. (2018) una investigación aplicada está basada en resultados de investigaciones básicas, la cual permiten formular problemas e hipótesis de trabajo teniendo como objetivo resolver diversos inconvenientes que acogen a la sociedad, región o país.

3.1.2 Diseño de investigación

El diseño de esta investigación fue no experimental del tipo transversal correlacional simple, ya que solo se observó en un tiempo determinado la correlación de las variables. Para Hernández et al. (2018) un estudio no experimental se trata de no manipular las variables, principalmente la independiente, debido a que se desea observar el efecto que tiene frente a la otra variable. En correlación, Hernández y Mendoza (2018) mencionan que, al ser de tipo transversal y corte correlacional, busca recopilar información en un tiempo determinado y probar una hipótesis para obtener a una conclusión mediante la justificación de las variables.

Esquema del diseño del estudio



1-Variable independiente: Gestión de la ciberseguridad

2-Variable dependiente: Concientización digital

3-R: Relación causal

3.2 Variables y operacionalización

- **Variable Independiente: Gestión de la ciberseguridad**

Esta variable independiente se catalogó como cuantitativa de tipo ordinal. Ñaupas (2018) menciona que la variable cuantitativa tiene como base principal medir las unidades que requieran resultados numéricos. Esto con la finalidad de generar una pretensión de análisis de los datos para contestar las interrogantes de un estudio. (Ver anexo 1)

- **Definición conceptual de la variable Gestión de la ciberseguridad**

Conforme a la Resolución peruana SBS N° 504-2021 (2021) menciona a la gestión de la seguridad de la información y ciberseguridad (SGSI-C) como una lista de reglas, procedimientos, técnicas, funciones y actividades diseñadas para identificar y resguardar los activos de información, identificar incidentes de seguridad, predecir respuestas y recuperarse de incidentes de ciberseguridad. (Ver anexo 1)

- **Definición operacional de la variable Gestión de la ciberseguridad**

Se particionó en 3 dimensiones: evaluación de riesgos, políticas de seguridad y supervisión de actividades; estas dimensiones serán medidas mediante un cuestionario, el cual empleará la escala de Likert aplicando 5 categorías: Totalmente en desacuerdo (1), En desacuerdo (2), Neutral (3), De acuerdo (4), Totalmente de acuerdo (5). (Ver anexo 1).

- **Indicadores**

De acuerdo a la primera dimensión Evaluación de riesgos se consideró los indicadores: exposición y detección; en la segunda dimensión Políticas de seguridad se consideró los indicadores: control y documentación; y en la tercera dimensión Supervisión de actividades se consideró los indicadores: monitoreo y análisis. (Ver anexo 1)

- **Escala de medición**

En consideración a la variable independiente Gestión de la ciberseguridad se planteó 12 preguntas en el cuestionario donde se empleó una medición ordinal. (Ver anexo 1)

- **Variable dependiente: Concientización digital**

Esta variable dependiente se catalogó como cuantitativa de tipo ordinal. Según, Cienfuegos et al. (2016) mencionan que la variable cuantitativa hace referencia a la escala numérica, por consiguiente, permite operaciones aritméticas y de medición. (Ver anexo 1)

- **Definición conceptual de la variable Concientización digital**

Según, Karakuş y Kılıç (2022) indican que la conciencia digital es una capacidad de conocer, apreciar y observar el entorno que rodea al individuo en afinidad al campo de las tecnologías digitales. (Ver anexo 1)

- **Definición operacional de la variable Concientización digital**

Se particionó en 3 dimensiones: conocimiento tecnológico, habilidad digital y seguridad digital; estas dimensiones serán medidas mediante un cuestionario, el cual empleará la escala de Likert aplicando 5 categorías: Totalmente en desacuerdo (1), En desacuerdo (2), Neutral (3), De acuerdo (4), Totalmente de acuerdo (5). (Ver anexo 1)

- **Indicadores**

De acuerdo a la dimensión Conocimiento tecnológico se consideró los indicadores: comprensión y usabilidad; en la dimensión Habilidad digital se consideró los indicadores: Competencia y evaluación; y en la dimensión Seguridad digital se consideró los indicadores: protección y prevención. (Ver anexo 1)

- **Escala de medición**

Para la variable dependiente Concientización digital se planteó 12 preguntas en el cuestionario donde se empleó una medición ordinal. (Ver anexo 1)

3.3 Población, muestra y muestreo, unidad de análisis

3.3.1 Población

La población considerada en esta investigación fue de 250 usuarios administrativos de una empresa Outsourcing, constituidas por 5 puestos diferentes, los cuales fueron: directorio, gerencia, subgerencia, jefes de área, supervisores, personal TI y colaboradores. Para Ñaupas et al. (2018) una población consta de un total de componentes de análisis, las cuales tienen que cumplir con ciertas características necesarias para ser incluidas. Estas pueden ser constituidas por personas, objetos, hechos o fenómenos. Así mismo, Arias et al. (2016) manifiestan que la población se trata de un conglomerado de asuntos, delimitaciones, determinaciones y viabilidades, las cuales permitirán la deliberación de la muestra de acuerdo a un acatamiento de criterios.

- **Criterios de inclusión**

Se consideró solo a los usuarios administrativos, quienes emplean como herramienta de trabajo un equipo informático, ya que este les permite tener acceso a los archivos y correos electrónicos de la organización.

- **Criterios de exclusión**

Se descartó a los usuarios que no usan un equipo informático para ejercer sus funciones laborales, ya que no tienen un medio de acceso a la red empresarial.

Tabla 1

Especificación de la población de una empresa Outsourcing

Población	Cantidad
Directorio	10
Gerencia	8
Subgerente	5
Jefes de área	15
Supervisores	10
Personal TI	9
Colaboradores	193
Total	250

Nota: Elaborado por el investigador

3.3.2 Muestra

La muestra en este estudio corresponde a 151 usuarios administrativos de una empresa Outsourcing. Este cálculo se realizó con la ayuda de la herramienta Decision Analyst STATS Versión 2.0, donde se consideró el 95% como nivel de confianza, un 5% de margen de error y una población de 250 usuarios. (Ver anexo 6). Para Ñaupas et al. (2018) una muestra es una proporción de la población, los cuales tienen que cumplir con ciertos aspectos exclusivos para el estudio. Adicionalmente, Sánchez (2018) menciona que una muestra es un compuesto de elementos o individuos pertenecientes a una población, donde se emplea métodos de muestreo probabilístico o no probabilístico.

Tabla 2

Detalle de la muestra de una empresa Outsourcing

Población	Cantidad
Directorio	5
Gerencia	5
Subgerente	3
Jefes de área	10
Supervisores	5
Personal TI	7
Colaboradores	116
Total	151

Nota: Elaborado por el investigador

3.3.3 Muestreo

Se empleó un muestreo probabilístico de tipo aleatorio simple, debido a que se tomó al azar a los usuarios administrativos de una empresa Outsourcing. Al respecto Hernández et al. (2018) sostienen que el muestreo está compuesto por partes de una población, los cuales permiten una mayor probabilidad aleatoria de ser escogida.

3.3.3 Unidad de análisis

Se consideró a los usuarios administrativos de una empresa Outsourcing.

3.4 Técnicas e instrumentos de recolección de datos

- **Técnica de recolección de datos**

En este estudio se usó como técnica la encuesta en línea empleando un formulario de Google. En concordancia con Hernández et al. (2018) señalan que

este procedimiento permite recolectar datos a través de varias interrogantes enfocadas a una o más variables de estudio con el propósito de poder medirlas.

- **Instrumento de recolección de datos**

Para este caso se usó un cuestionario como herramienta. (Ver Anexo 2). Hernández et al. (2018) señalan que los cuestionarios pueden estar compuestos por preguntas abiertas y/o cerradas sobre las variables a estudiar, siendo de esta forma el instrumento más empleado para la recopilación de datos.

Tabla 3

Herramienta de medición

Dato del instrumento	Cuestionario para usuarios administrativos de una empresa Outsourcing
1- Autor:	Angeles Gonzales, Edwin Ivan
2- Año:	2023
3- Tipo de instrumento	Cuestionario
4- Objetivo	Determinar la influencia de la gestión de la ciberseguridad en la concientización digital en los usuarios administrativos de una empresa Outsourcing, Lima 2023
5- Población	250 trabajadores de una empresa Outsourcing
6- Numero de ítems	24 en total dividido en V.I (12) y V.D (12)
7- Aplicación	En línea
8- Tiempo utilizado	15 minutos
9- Escala	Escala de Likert: Totalmente en desacuerdo (1), En desacuerdo (2), Neutral (3), De acuerdo (4), Totalmente de acuerdo (5). (Ver anexo 2).
10- Niveles y Rangos	Óptimo (del 45 al 60)
	Regular (del 29 al 44)
	Deficiente (del 12 al 28)

Nota: Elaborado por el investigador

- **Validez**

En este caso dicha validez del instrumento se realizó con apoyo de la evaluación de tres catedráticos de la UCV mediante el juicio de expertos donde se determinó diversos criterios como la claridad, coherencia y por último el valor de cada pregunta del cuestionario. (Ver Anexo 3). Al respecto, Hernández et al. (2018) indican que la validez es un rango del instrumento que evalúa a la variable de estudio que se pretende medir con la finalidad de probar si es adecuada.

Tabla 4

Determinación del juicio de expertos

DNI	Experto	Procedencia	Calificación
42097456	Acuña Benites, Marlon Frank	UCV	Aplicable
06809706	Espinoza Espinoza, Alindor Fernando	UCV	Aplicable
18167212	Pacheco Torres, Juan Francisco	UCV	Aplicable

Nota: Elaborado por el investigador

- **Confiabilidad**

En este estudio se usó Alfa de Cronbach para demostrar la confiabilidad del instrumento; en la primera fase se ejecutó una prueba piloto de 50 encuestas para probar la confiabilidad, donde se obtuvo como resultado 0.973 de Alfa de Cronbach. Para la segunda fase se consideró a la totalidad de la muestra de 151 encuestas arrojando un resultado de confiabilidad de 0.978 de Alfa de Cronbach. De este modo se resolvió que el instrumento de este estudio es altamente confiable. (Ver anexo 7). Hernández et al. (2018) manifiestan que el rango en un uso repetido de una constante es aplicado a la misma persona u objeto produciendo así, el mismo resultado.

Figura 1

Rangos Alfa de Cronbach

Rangos de α	Magnitud de confiabilidad
0.81 a 1.00	*Muy alta*
0.61 a 0.80	*Alta*
0.41 a 0.60	*Moderada*
0.21 a 0.40	*Baja*
0.01 a 0.20	*Muy baja*

Nota: Ruiz (2013)

3.5 Procedimientos

Respecto a la recolección de la información en este estudio se realizó de la siguiente manera: primero se elaboró el instrumento del cuestionario de 24 preguntas relacionadas a las variables de estudio y sus respectivas dimensiones e indicadores. Segundo se validó el instrumento mediante el juicio de expertos con apoyo de los catedráticos del posgrado de la UCV, donde evaluaron los principios de claridad, ilación y valoración de cada pregunta del cuestionario. Tercero se analizó la confiabilidad de los resultados con la herramienta SPSS versión 29 aplicando Alfa de Cronbach, donde primero se aplicó un piloto a 50 usuarios administrativos y luego a 151 usuarios administrativos, obteniendo como resultado en ambas pruebas una alta confiabilidad. Por último, se aplicó un análisis descriptivo e inferencial para contrastar las hipótesis esbozadas de la investigación.

3.6 Método de análisis de datos

En el aspecto descriptivo e inferencial en este estudio se empleó la herramienta estadística IBM SSPS Versión 29.0.1.0 y también Microsoft Excel para la ayuda del análisis y gráficos. En el análisis estadístico se usó una prueba de normalidad Kolmogorov-Smirnov, el coeficiente de correlación Rho Spearman por ser no paramétrico, el modelo de R cuadrado y ANOVA.

3.7 Aspectos éticos

Este estudio estuvo alineado al reglamento de código de ética de la Universidad Cesar Vallejo dispuesto por la Resolución de Consejo Universitario Nº0470-2022-UCV.

Respecto a la propiedad intelectual se respetó la autoría de los investigadores que se tomó como referencia, los cuales por normativa fueron citados según la norma APA - 7.

Respecto a la autonomía en esta investigación se consideró la voluntad del empleado en la participación de la encuesta mediante un modelo de consentimiento informado. (Ver anexo 3)

IV. RESULTADOS

En correlación al objetivo general de la investigación: la gestión de la ciberseguridad influye significativamente en la concientización digital en los usuarios administrativos de una empresa Outsourcing, Lima 2023. Se realizó el análisis descriptivo de la variable Gestión de la ciberseguridad y la variable concientización digital.

Tabla 5

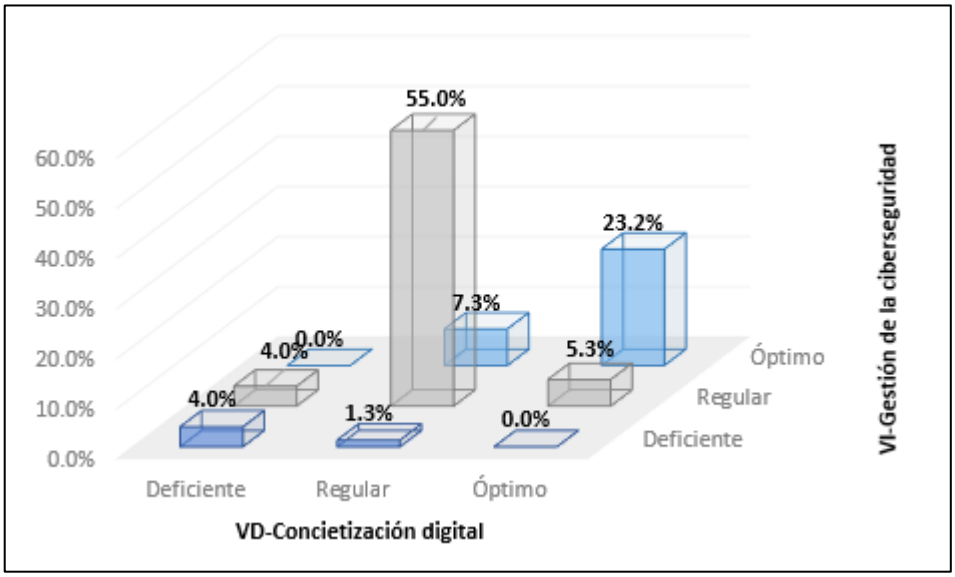
*Tabla cruzada: V.I-Gestión de la ciberseguridad * V.D-Concientización digital*

		VD-Concientización digital							
		Deficiente		Regular		Óptimo		Total	
		N	%	N	%	N	%	N	%
VI-Gestión de la ciberseguridad	Deficiente	6	4.0%	2	1.3%	0	0.0%	8	5.3%
	Regular	6	4.0%	83	55.0%	8	5.3%	97	64.2%
	Óptimo	0	0.0%	11	7.3%	35	23.2%	46	30.5%
Total		12	7.9%	96	63.6%	43	28.5%	151	100.0%

Nota: Elaborado por el investigador con asistencia de SPSS V29.

Figura 2

*Histograma: VI-Gestión de la ciberseguridad * VD-Concientización digital*



Nota: Elaborado por el investigador con apoyo de MS Excel.

En función al histograma de la figura 2, se visualiza que el mayor valor de frecuencia se manifiesta en el grado “Regular” de la variable Gestión de la ciberseguridad y el grado “Regular” de la variable Concientización digital, obteniendo 83 respuestas equivalente al 55.0% de la totalidad. Como valor intermedio se obtuvo el grado “Óptimo” de la variable Gestión de la ciberseguridad y el grado “Óptimo” de la variable Concientización digital, obteniendo 35 respuestas equivalente al 23.2% de la totalidad. Como menor valor se obtuvo el grado “Óptimo” de la variable Gestión de la ciberseguridad y el grado “Deficiente” de la variable Concientización digital; y el grado “Deficiente” de la variable Gestión de la ciberseguridad y el grado “Óptimo” de la variable Concientización digital, obteniendo en ambos casos 0 respuestas equivalente al 0.0% de la totalidad. Respecto a la tabla 5 las frecuencias más altas fueron el grado “Regular” de la variable Gestión de la ciberseguridad, obteniendo 97 respuestas equivalente al 64.2% de la totalidad y el grado “Regular” de la variable Concientización digital, obteniendo 96 respuestas equivalente al 63.6% de la totalidad.

- **Verificación de hipótesis**

Se formula la siguiente hipótesis general para este estudio como parte del análisis inferencial:

$H\text{-}_0$: La gestión de la ciberseguridad influye significativamente en la concientización digital en los usuarios administrativos de una empresa Outsourcing, Lima 2023.

$H\text{-}_1$: La gestión de la ciberseguridad no influye significativamente en la concientización digital en los usuarios administrativos de una empresa Outsourcing, Lima 2023.

Tabla 6

Normalidad - Kolmogorov-Smirnov– SV1 / SV2

	Estadístico	gl	Sig.
SV1	.132	151	<.001
SV2	.117	151	<.001

Nota: Elaborado por el investigador con apoyo de SPSS V29

Respecto a la tabla 6 se empleó la prueba de normalidad en este caso Kolmogorov-Smirnov, debido a que la muestra fue mayor a 50 encuestas entre la variable independiente Gestión de la ciberseguridad y la variable dependiente Concientización digital donde resultó que el valor de $p < 0.001$ en ambas variables. Demostrando así, ser menor al 0.05 estipulado como normal, por lo tanto, se consideró como una distribución no paramétrica debido a que no presenta normalidad.

Tabla 7

Correlación - Rho Spearman SV1 / SV2

		SV1	SV2
SV1	Coeficiente de correlación	1.000	.847**
	Sig. (bilateral)	.	<.001
	N	151	151
SV2	Coeficiente de correlación	.847**	1.000
	Sig. (bilateral)	<.001	.
	N	151	151

Nota: Elaborado por el investigador con apoyo de SPSS V29

Respecto a la tabla 7 se empleó el coeficiente de correlación de Rho Spearman, ya que la distribución es no paramétrica. Esta correlación arrojó un resultado de 0.847 para ambas variables y un valor $p < 0.001$, por consiguiente, se acepta la hipótesis nula ($H\text{-}_0$), considerando así la existe de una vinculación positiva alta y una relación significativa entre la variable independiente Gestión de la ciberseguridad y la variable dependiente Concientización digital.

Figura 3

Valor de Rho Spearman

Valor de *rho*	Significado
-1	Correlación negativa grande y perfecta
-0.9 a -0.99	Correlación negativa muy alta
-0.7 a -0.89	Correlación negativa alta
-0.4 a -0.69	Correlación negativa moderada
-0.2 a -0.39	Correlación negativa baja
-0.01 a -0.19	Correlación negativa muy baja
0	Correlación nula
0.01 a 0.19	Correlación positiva muy baja
0.2 a 0.39	Correlación positiva baja
0.4 a 0.69	Correlación positiva moderada
0.7 a 0.89	Correlación positiva alta
0.9 a 0.99	Correlación positiva muy alta
1	Correlación positiva grande y perfecta

Nota: Martínez et al. (2015)

Respecto al primer objetivo específico que fue determinar la influencia de la dimensión evaluación de riesgos de la gestión de la ciberseguridad en la concientización digital en los usuarios administrativos de una empresa Outsourcing, Lima 2023. Se realizó el análisis descriptivo de la dimensión Evaluación de riesgos de la Gestión de la ciberseguridad y la variable Concientización digital.

Tabla 8

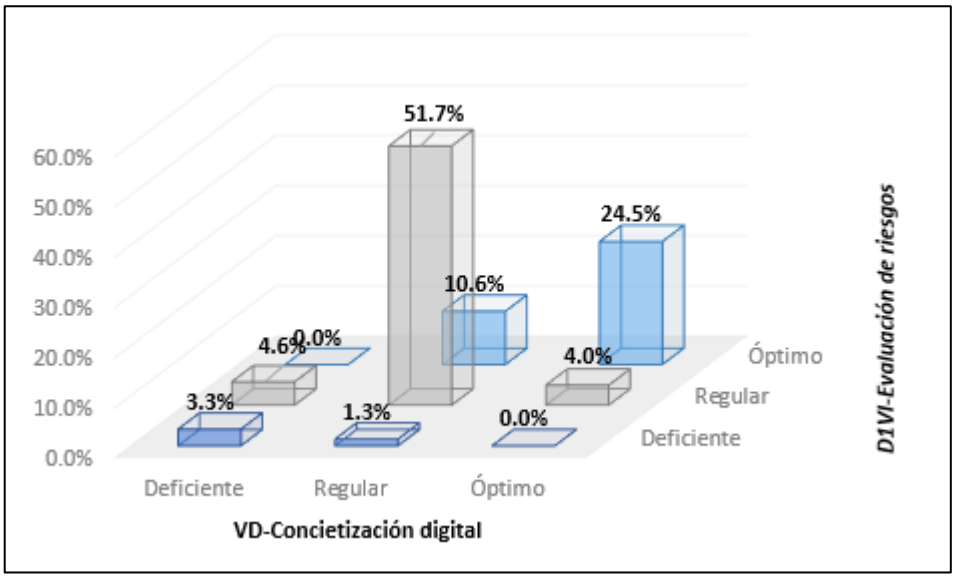
*Tabla cruzada: D1.V.I-Evaluación de riesgos * V.D-Concientización digital*

		VD-Concientización digital							
		Deficiente		Regular		Optimo		Total	
		N	%	N	%	N	%	N	%
D1VI-Evaluación de riesgos	Deficiente	5	3.3%	2	1.3%	0	0.0%	7	4.6%
	Regular	7	4.6%	78	51.7%	6	4.0%	91	60.3%
	Optimo	0	0.0%	16	10.6%	37	24.5%	53	35.1%
Total		12	7.9%	96	63.6%	43	28.5%	151	100.0%

Nota: Elaborado por el investigador con asistencia de SPSS V29.

Figura 4

*Histograma: D1VI-Evaluación de riesgos * VD-Concientización digital*



Nota: Elaborado por el investigador con apoyo de MS Excel.

En función a la figura 4, se observa que el mayor valor de la frecuencia se manifiesta en el grado “Regular” de la dimensión Evaluación de riesgos de la Gestión de la ciberseguridad y el grado “Regular” de la variable Concientización digital, obteniendo 78 respuestas equivalente al 51.7% de la totalidad. Como valor intermedio se obtuvo el grado “Óptimo” de la dimensión Evaluación de riesgos de la Gestión de la ciberseguridad y el grado “Óptimo” de la variable Concientización digital, obteniendo 37 respuestas equivalente al 24.5% de la totalidad. Como menor valor se obtuvo el grado “Óptimo” de la dimensión Evaluación de riesgos de la Gestión de la ciberseguridad y el grado “Deficiente” de la variable Concientización digital; y el grado “Deficiente” de la dimensión Evaluación de riesgos de la Gestión de la ciberseguridad y el grado “Óptimo” de la variable Concientización digital, obteniendo 0 respuestas equivalente al 0.0% de la totalidad. Respecto a la tabla 8 las frecuencias más altas fueron el grado “Regular” de la dimensión Evaluación de riesgos de la Gestión de la ciberseguridad, obteniendo 91 respuestas equivalente al 60.3% de la totalidad y el grado “Regular” de la variable Concientización digital, obteniendo 96 respuestas equivalente al 63.6% de la totalidad.

- **Verificación de hipótesis especifica 1**

Se formula la siguiente hipótesis específica para esta investigación como parte del análisis inferencial:

H-$_0$: La dimensión evaluación de riesgos de la gestión de la ciberseguridad influye significativamente en la concientización digital en los usuarios administrativos de una empresa Outsourcing, Lima 2023

H-$_1$: La dimensión evaluación de riesgos de la gestión de la ciberseguridad no influye significativamente en la concientización digital en los usuarios administrativos de una empresa Outsourcing, Lima 2023.

Tabla 9

Normalidad - Kolmogorov-Smirnov– SD1 / SV2

	Estadístico	gl	Sig.
SD1	.156	151	<.001
SV2	.117	151	<.001

Nota: Elaborado por el investigador con apoyo de SPSS V29

Respecto a la tabla 9 se aplicó la prueba de normalidad en este caso Kolmogorov-Smirnov, debido a que la muestra fue mayor a 50 encuestas entre la dimensión Evaluación de riesgos de la Gestión de la ciberseguridad y la variable dependiente Concientización digital donde resultó que el valor de $p < 0.001$ en ambas variables. Demostrando así, ser menor al 0.05 estipulado como normal, por lo tanto, se consideró como una distribución no paramétrica debido a que no presenta normalidad.

Tabla 10

Correlación - Rho Spearman D1 / SV2

		SV1	SV2
SD1	Coeficiente de correlación	1.000	.818**
	Sig. (bilateral)	.	<.001
	N	151	151
SV2	Coeficiente de correlación	.818**	1.000
	Sig. (bilateral)	<.001	.
	N	151	151

Nota: Elaborado por el investigador con apoyo de SPSS V29

Respecto a la tabla 10 se empleó el coeficiente de correlación de Rho Spearman, ya que la distribución es no paramétrica. Esta correlación arrojó un resultado de 0.818 para ambas variables y un valor $p < 0.001$, por consiguiente, se acepta la hipótesis nula (H_0), considerando así la existe de una vinculación positiva alta y una relación significativa entre la dimensión Evaluación de riesgos de la Gestión de la ciberseguridad y la variable dependiente Concientización digital.

Respecto al segundo objetivo específico que fue determinar la influencia de la dimensión políticas de seguridad de la gestión de la ciberseguridad en la concientización digital en los usuarios administrativos de una empresa Outsourcing, Lima 2023. Se realizó un análisis descriptivo de la dimensión Políticas de seguridad de la Gestión de la ciberseguridad y la variable Concientización digital.

Tabla 11

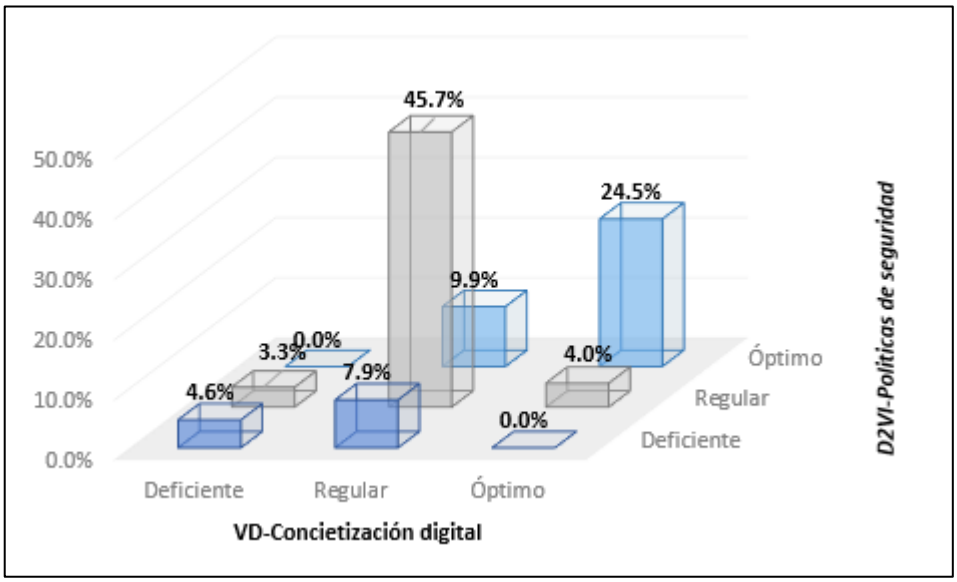
*Tabla cruzada: D2.V.I-Politicas de seguridad * V.D-Concientización digital*

		VD-Concientización digital							
		Deficiente		Regular		Optimo		Total	
		N	%	N	%	N	%	N	%
D2VI-Politicas de seguridad	Deficiente	7	4.6%	12	7.9%	0	0.0%	19	12.6%
	Regular	5	3.3%	69	45.7%	6	4.0%	80	53.0%
	Optimo	0	0.0%	15	9.9%	37	24.5%	52	34.4%
Total		12	7.9%	96	63.6%	43	28.5%	151	100.0%

Nota: Elaborado por el investigador con asistencia de SPSS V29.

Figura 5

*Histograma: D2VI-Politicas de seguridad * VD-Concientización digital*



Nota: Elaborado por el investigador con apoyo de MS Excel.

En función a la figura 5, se observa que el mayor valor de la frecuencia se manifiesta en el grado “Regular” de la dimensión Políticas de seguridad de la Gestión de la ciberseguridad y el grado “Regular” de la variable Concientización digital, obteniendo 69 respuestas equivalente al 45.7% de la totalidad. Como valor intermedio se obtuvo el grado “Óptimo” de la dimensión Políticas de seguridad de la Gestión de la ciberseguridad y el grado “Óptimo” de la variable de la Concientización digital, obteniendo 37 respuestas equivalente al 24.5% de la totalidad. Como menor valor se obtuvo el grado “Óptimo” de la dimensión Políticas de seguridad de la Gestión de la ciberseguridad y el grado “Deficiente” de la variable Concientización digital; y el grado “Deficiente” de la dimensión Políticas de seguridad de la Gestión de la ciberseguridad y el grado “Óptimo” de la variable Concientización digital, obteniendo en ambos casos 0 respuestas equivalente al 0.0% de la totalidad. Respecto a la tabla 11 las frecuencias más altas fueron el grado “Regular” de la dimensión Políticas de seguridad de la Gestión de la ciberseguridad, obteniendo 80 respuestas equivalente al 53.0% de la totalidad y el grado “Regular” de la variable Concientización digital, obteniendo 96 respuestas equivalente al 63.6% de la totalidad.

- **Verificación de hipótesis especifica 2**

Se formula la siguiente hipótesis específica para esta investigación como parte del análisis inferencial:

H-$_0$: La dimensión política de seguridad de la gestión de la ciberseguridad influye significativamente en la concientización digital en los usuarios administrativos de una empresa Outsourcing, Lima 2023.

H-$_1$: La dimensión política de seguridad de la gestión de la ciberseguridad no influye significativamente en la concientización digital en los usuarios administrativos de una empresa Outsourcing, Lima 2023.

Tabla 12

Normalidad - Kolmogorov-Smirnov– SD2 / SV2

	Estadístico	gl	Sig.
SD2	.116	151	<.001
SV2	.117	151	<.001

Nota: Elaborado por el investigador con apoyo de SPSS V29

Respecto a la tabla 12 se aplicó la prueba de normalidad en este caso Kolmogorov-Smirnov, debido a que la muestra fue mayor a 50 encuestas entre la dimensión Política de seguridad de la Gestión de la ciberseguridad y la variable dependiente Concientización digital donde resultó que el valor de $p < 0.001$ en ambas variables. Demostrando así, ser menor 0.05 estipulado como normal, por lo tanto, se consideró como una distribución no paramétrica debido a que no presenta normalidad.

Tabla 13

Correlación - Rho Spearman D2 / SV2

		SV1	SV2
SD2	Coeficiente de correlación	1.000	.823**
	Sig. (bilateral)	.	<.001
	N	151	151
SV2	Coeficiente de correlación	.823**	1.000
	Sig. (bilateral)	<.001	.
	N	151	151

Nota: Elaborado por el investigador con apoyo de SPSS V29

Respecto a la tabla 13 se empleó el coeficiente de correlación de Rho Spearman, ya que la distribución es no paramétrica. Esta correlación arrojó un resultado de 0.823 para ambas variables y un valor $p < 0.001$, por consiguiente, se acepta la hipótesis nula (H_0), considerando así la existe de una vinculación positiva alta y una relación significativa entre la dimensión Política de riesgo de la Gestión de la ciberseguridad y la variable dependiente Concientización digital.

Respecto al tercer objetivo específico que fue determinar la influencia de la dimensión supervisión de actividades de la gestión de la ciberseguridad en la concientización digital en los usuarios administrativos de una empresa Outsourcing, Lima 2023. Se realizó el análisis descriptivo de la dimensión Supervisión de actividades de la Gestión de la ciberseguridad y la variable Concientización digital.

Tabla 14

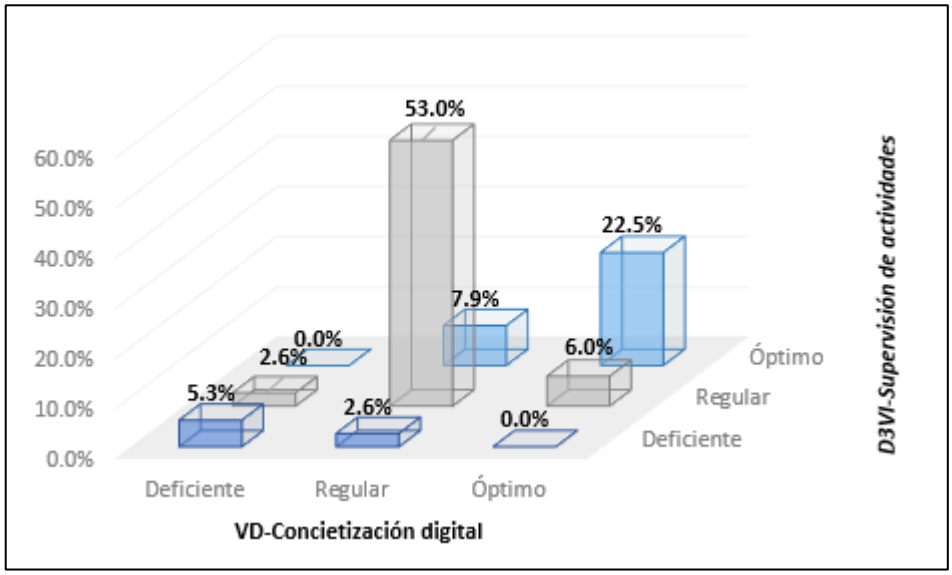
*Tabla cruzada: D3.V.I-Supervisión de actividades * V.D-Concientización digital*

		VD-Concientización digital							
		Deficiente		Regular		Optimo		Total	
		N	%	N	%	N	%	N	%
D3VI-Supervisión de actividades	Deficiente	8	5.3%	4	2.6%	0	0.0%	12	7.9%
	Regular	4	2.6%	80	53.0%	9	6.0%	93	61.6%
	Optimo	0	0.0%	12	7.9%	34	22.5%	46	30.5%
Total		12	7.9%	96	63.6%	43	28.5%	151	100.0%

Nota: Elaborado por el investigador con asistencia de SPSS V29.

Figura 6

*Histograma: D3VI-Supervisión de actividades * VD-Concientización digital*



Nota: Elaborado por el investigador con apoyo de MS Excel.

En a la figura 6, se observa que el mayor valor de la frecuencia se manifiesta en el grado “Regular” de la dimensión Supervisión de actividades de la Gestión de la ciberseguridad y el grado “Regular” de la variable Concientización digital, obteniendo 80 respuestas equivalente al 53.0% de la totalidad. Como valor intermedio se obtuvo el grado “Óptimo” de la dimensión Supervisión de actividades de la Gestión de la ciberseguridad y el grado “Óptimo” de la variable Concientización digital, obteniendo 34 respuestas equivalente al 22.5% de la totalidad. Como menor valor se obtuvo el grado “Óptimo” de la dimensión Supervisión de actividades de la Gestión de la ciberseguridad y el grado “Deficiente” de la variable Concientización digital; y el grado “Deficiente” de la dimensión Supervisión de actividades de la Gestión de la ciberseguridad y el grado “Óptimo” de la variable Concientización digital, obteniendo 0 respuestas equivalente al 0.0% de la totalidad. Respecto a la tabla 14 las frecuencias más altas fueron el grado “Regular” de la dimensión Supervisión de actividades de la Gestión de la ciberseguridad, obteniendo 93 respuestas equivalente al 61.6% de la totalidad y el grado “Regular” de la variable Concientización digital, obteniendo 96 respuestas equivalente al 63.6% de la totalidad.

- **Verificación de hipótesis especifica 3**

Se formula la siguiente hipótesis específica para esta investigación como parte del análisis inferencial:

$H\text{-}_0$: La dimensión supervisión de actividades de la gestión de la ciberseguridad influye significativamente en la concientización digital en los usuarios administrativos de una empresa Outsourcing, Lima 2023

$H\text{-}_1$: La dimensión supervisión de actividades de la gestión de la ciberseguridad no influye significativamente en la concientización digital en los usuarios administrativos de una empresa Outsourcing, Lima 2023.

Tabla 15

Normalidad - Kolmogorov-Smirnov– SD3 / SV2

	Estadístico	gl	Sig.
SD2	.180	151	<.001
SV2	.117	151	<.001

Nota: Elaborado por el investigador con apoyo de SPSS V29

Respecto a la tabla 15 se aplicó la prueba de normalidad en este caso Kolmogorov-Smirnov, debido a que la muestra fue mayor a 50 encuestas entre la dimensión Supervisión de actividades de la Gestión de la ciberseguridad y la variable dependiente Concientización digital donde resultó que el valor de $p < 0.001$ en ambas variables. Demostrando así, ser menor 0.05 estipulado como normal, por lo tanto, se consideró como una distribución no paramétrica debido a que no presenta normalidad.

Tabla 16

Correlación - Rho Spearman D3 / SV2

		SV1	SV2
SD3	Coeficiente de correlación	1.000	.818**
	Sig. (bilateral)	.	<.001
	N	151	151
SV2	Coeficiente de correlación	.818**	1.000
	Sig. (bilateral)	<.001	.
	N	151	151

Nota: Elaborado por el investigador con apoyo de SPSS V29

Respecto a la tabla 16 se empleó el coeficiente de correlación de Rho Spearman, ya que la distribución es no paramétrica. Esta correlación arrojó un resultado de 0.818 para ambas variables y un valor $p < 0.001$, por consiguiente, se acepta la hipótesis nula (H_0), considerando así la existe de una vinculación positiva alta y una relación significativa entre la dimensión Supervisión de actividades de la Gestión de la ciberseguridad y la variable dependiente Concientización digital.

- **Prueba de regresión lineal**

Tabla 17

Estadísticos descriptivos

	Media	Desv. estándar	N
SV2	38.07	8.134	151
SV1	39.07	7.688	151

Nota: Elaborado por el investigador con asistencia de SPSS V29

Respecto a la tabla 17 se reflejó índices de la Media, Desviación estándar de la Gestión de la ciberseguridad y la variable Concientización digital de un total de muestra de 151 encuestas.

Tabla 18

Modelo-R

Modelo	R	R cuadrado	R cuadrado ajustado	Error estándar de la estimación
1	.869[a]	.755	.754	4.036

Nota: Elaborado por el investigador con asistencia de SPSS V29

Respecto a la tabla 18 se reflejó el modelo del R cuadrado con un 75.5% aproximándose al valor 1 de un ajuste perfecto. Respecto al R cuadrado ajustado presentó un ajuste lineal de 75.4 % en ambas variables, lo cual indica que es fiable para previsiones futuras.

Tabla 19

Modelo-ANOVA

Modelo		Suma de cuadrados	gl	Media cuadrática	F	Sig.
1	Regresión	7496.559	1	7496.559	460.113	<.001[b]
	Residuo	2427.639	149	16.293		
	Total	9924.199	150			

Nota: Elaborado por el investigador con asistencia de SPSS V29

Respecto a la tabla 19 se reflejó que la varianza del modelo ANOVA presentó un enlace significativo para ambas variables, por lo tanto, corroboró la aceptación de H_0 planteada en el estudio.

V. DISCUSIÓN

En correlación con el objetivo general, los resultados de este estudio en el análisis descriptivo arrojaron que la frecuencia más alta obtenida fue en el grado regular de la Gestión de la ciberseguridad en conjunto con el grado regular de la Concientización digital, obteniendo 83 respuestas representadas equivalentemente al 55% del total de encuestas realizadas a los usuarios administrativos de una empresa Outsourcing. A diferencia de la menor frecuencia encontrada en el grado óptimo de la Gestión de la ciberseguridad con el grado deficiente de la Concientización digital y el grado deficiente de la Gestión de la ciberseguridad con el grado óptimo de la Concientización digital donde en ambos casos no se obtuvieron respuestas.

Los resultados de las estadísticas del análisis inferencial arrojaron en la comprobación de normalidad un valor de $p < 0.001$ en ambas variables, por lo que demuestra que la distribución obtenida es no paramétrica. Consecuentemente, se empleó el Rho de Spearman para resolver el nivel de correlación de las variables obteniendo así, un resultado de 0.847 dando un grado de vinculación positiva alta y respecto al valor $p < 0.001$ la existencia de una significancia entre la Gestión de la ciberseguridad y la concientización digital. De este modo se da por entendido la aprobación de la hipótesis nula planteada en esta investigación.

En las investigaciones mencionadas con anterioridad se encuentran la de Fadlika et al. (2023) en su estudio sobre la concientización en la seguridad de la información a los usuarios del sector de energía realizado en Indonesia, sostuvo como objetivo calcular el grado de concientización de la seguridad de la información, con ello investigar la correlación entre el conocimiento, actitud y conducta del personal de la empresa y como conclusión demostraron la existencia de una alta conciencia en la seguridad de la información, mientras que, en otros aspectos como el uso de internet, manejo de información y gestión de activos requieren mejorar la concientización. Referente al estudio presentado se demuestra una vinculación de la concientización con la seguridad de la información, algo similar como se obtuvo con la gestión de la ciberseguridad. Del mismo modo, Krawczyk y Caputa (2023) en el estudio sobre la conciencia de la seguridad de la red y perspectiva del cliente realizado en Polonia, tuvo como objetivo evaluar la

conciencia de seguridad en la red entre el cliente y empresa y como conclusión del estudio determinó que el grado de conciencia de seguridad de red de los usuarios presenta una falsa convicción debido, a que se sobreestiman las habilidades digitales de percepción, acción y conocimiento de los usuarios. Referente al estudio presentado se demuestra la vinculación de la concientización con la seguridad a un mejor nivel en el conocimiento de los usuarios a diferencia a lo encontrado en la investigación con la gestión de la ciberseguridad. Así también, Khan et al. (2023) en el estudio sobre la evaluación de la motivación de protección apoyada en la capacitación de concientización sobre seguridad cibernética empleando el modelo Kirkpatrick realizado en Pakistán, tuvo como objetivo comprender el comportamiento después de la implementación del entrenamiento en ciberseguridad y como conclusión fue que la capacitación en ciberseguridad incrementó significativamente la autoeficacia de los estudiantes y contribuyó con la concientización en ciberseguridad. De igual manera Akter et al. (2022) en el estudio sobre la competencia de concienciación sobre la ciberseguridad en una economía digital realizada en Australia, cuyo objetivo fue identificar las dimensiones de las capacidades de concienciación sobre la ciberseguridad en una organización en una economía digital basada en datos y como conclusión fue que el desarrollo de la Concientización sobre las Capacidades de Ciberseguridad (CSAC) puede ser empleada en diversas organizaciones específicas, pero que cuenten con la interacción y compromiso de los usuarios finales. De la misma forma Datt y Tewari (2021) en el estudio sobre la actitud y conciencia de los usuarios hacia la seguridad cibernética realizado en la India, tuvieron como objetivo analizar las actitudes y conciencia de los usuarios frente a la ciberseguridad clasificados por el género, estado laboral y calificaciones y como conclusión determinaron que más del 85% del personal cuenta con habilidades en TI. Dichas habilidades se miden con los siguientes criterios: fundamentos de TI, aplicaciones básicas de oficina y habilidades de internet, pero un escaso nivel de concientización de la seguridad cibernética.

En relación con las definiciones de la Gestión de la ciberseguridad la Resolución peruana SBS N° 504-2021 (2021) menciona a la gestión de la seguridad de la información y ciberseguridad (SGSI-C) como una lista de reglas, procedimientos, técnicas, funciones y actividades diseñadas para identificar y

resguardar los activos de información, identificar incidentes de seguridad, predecir respuestas y recuperarse de incidentes de ciberseguridad.

Concerniente al objetivo específico 1, los resultados de este estudio en el análisis descriptivo arrojaron que la frecuencia más alta obtenida fue en el grado regular en la dimensión Evaluación de riesgos de la Gestión de la ciberseguridad en conjunto con el grado regular de la Concientización digital, obteniendo 78 respuestas representadas equivalentemente al 51.7% del total de encuestas realizadas a los usuarios administrativos de una empresa Outsourcing. A diferencia de la menor frecuencia encontrada en el grado óptimo de la dimensión Evaluación de riesgos de la Gestión de la ciberseguridad con el grado deficiente de la Concientización digital y el grado deficiente de la dimensión Evaluación de riesgos de la Gestión de la ciberseguridad con el grado óptimo de la Concientización digital donde en ambos casos no se obtuvieron respuestas.

Los resultados estadísticos del análisis inferencial arrojaron en la comprobación de normalidad un valor de $p < 0.001$ para la dimensión uno en ambas variables, por lo que demuestra que la distribución es no paramétrica. Por ende, se empleó Rho de Spearman para resolver el grado de correlación de las variables obteniendo así un resultado de 0.818, dando un grado de vinculación positiva alta y respecto al p valor < 0.001 demostrando la existencia de una significancia entre la dimensión Evaluación de riesgos de la Gestión de la ciberseguridad y la concientización digital. De este modo se da por entendido la aprobación de la hipótesis nula planteada en este estudio.

En las investigaciones mencionadas con anterioridad se encuentran la de Boto-García (2023) en su estudio sobre la concienciación y formación del personal frente a los ciberataques y riesgos digitales en España, consideró como objetivo estudiar la relación de la concienciación y la formación de los empleados de una hostelería respecto a los temas de ciberdelincuencia y ciberataques en una entidad y como conclusión se determinó que las capacitaciones brindadas por las Pymes sobre ciberseguridad no están siendo efectivas, debido a que la diferencia detectada entre el personal capacitado y sin capacitar es mínima dejando de esta manera algunas brechas de seguridad que afectan a la empresa. Así mismo, Mendivil et al. (2022) en el estudio sobre la concienciación cibernética frente

amenazas y vulnerabilidades realizado en España, tuvo como objetivo estudiar el uso de modelos de aptitudes en programas de instrucción y concientización en ciberseguridad enfocados a los usuarios no TIC de una organización y como conclusión fue que el grado de aptitudes en las acciones de instrucción y concienciación de la ciberseguridad aplicada en los usuarios no TIC de una organización son muy escasos, además que las metodologías empleadas al parecer son suficientes, pues no parecen ser revisadas ni actualizadas. De forma similar, Huraj et al. (2023) en el estudio sobre Medición de la conciencia de seguridad cibernética entre estudiantes de computación y ciencia de medios realizado en Eslovaquia, tuvo como objetivo examinar las actitudes y conciencia de los estudiantes universitarios sobre la ciberseguridad y como conclusión fue que los estudiantes de la Ciencia de Computación y los estudiantes de la Ciencia de Medios presentan casi una misma actitud de conciencia frente a los problemas de ciberseguridad dando una ligera diferencia con los que tienen formación en informática.

En relación con las definiciones de la dimensión Evaluación de riesgos de la Gestión de la ciberseguridad Pinzón (2014) señala que es un proceso de identificación, análisis y valoración donde permite establecer un grado de amenaza y riesgo asociado teniendo en consideración el resultado del proceso y la identificación de los controles adecuados. En concordancia, Główczyńska (2010) menciona que la evaluación de riesgos consiste en una serie de procesos lógicos diseñados para analizar y evaluar sistemáticamente los peligros potenciales para la seguridad o la salud. Adicionalmente, De Freitas (2009) señala que la evaluación de riesgos es un procedimiento de estimación de riesgos y criterios establecidos, teniendo la finalidad de determinar el grado de importancia en una organización que desea contemplar un Sistema de Gestión de la Seguridad de la Información.

Correspondiente al objetivo específico 2, los resultados de esta investigación en el análisis descriptivo arrojaron que la frecuencia más alta obtenida fue en el grado regular en la dimensión Políticas de seguridad de la Gestión de la ciberseguridad en conjunto con el grado regular de la Concientización digital, obteniendo 69 respuestas representadas equivalentemente al 45.7% del total de encuestas realizadas a los usuarios administrativos de una empresa Outsourcing.

A diferencia de la menor frecuencia encontrada en el grado óptimo de la dimensión Políticas de seguridad de la Gestión de la ciberseguridad con el nivel deficiente de la Concientización digital y el grado deficiente de la dimensión Políticas de seguridad de la Gestión de la ciberseguridad con el grado óptimo de la Concientización digital donde en ambos casos no se obtuvieron respuestas.

Los resultados estadísticos del análisis inferencial arrojaron en la comprobación de la normalidad un valor de $p < 0.001$ en la dimensión dos de ambas variables, por lo que demuestra que la distribución es no paramétrica. Por ende, se empleó Rho de Spearman para resolver el grado de correlación de las variables obteniendo así un resultado de 0.823, dando un grado de vinculación positiva alta y respecto al p valor < 0.001 demostrando la existencia de una significancia entre la dimensión Políticas de seguridad de la Gestión de la ciberseguridad y la concientización digital. De este modo se da por entendido la aprobación de la hipótesis nula trazada en este estudio.

En las investigaciones mencionadas con anterioridad se encuentran la de Nwankpa y Datta (2023) con el estudio que se enfoca en los roles de la conciencia cibernética y políticas de seguridad realizado en los EE. UU, cuyo objetivo fue explorar cómo el trabajo remoto influye respecto a la conciencia de seguridad cibernética de los empleados y a la toma de precauciones en la seguridad y como conclusión fue que la capacitación, educación y gobernanza sobre la conciencia en ciberseguridad influye de forma positiva manifestando comportamientos autorregulados en los usuarios. De forma similar Reeves et al. (2023) realizo un estudio sobre las percepciones de los empleados sobre la seguridad cibernética, cuyo objetivo fue abordar la brecha de percepción y respuestas de los empleados frente a la observación de videos de ciberseguridad y como conclusión se obtuvo que los dos estudios se ubican entre los primeros en combinar la técnica Repertory Grid de Personal Construct Psychology (PCP) para un análisis hibrido deductivo e inductivo de respuesta de los empleados sobre el programa de Educación, Capacitación y Concientización sobre Seguridad (SETA) apoyados en los resultados de CAFS para la capacitación en seguridad cibernética. Así mismo, Tejay y Mohammed (2023) en el estudio orientado a una cultura de seguridad para el éxito sobre la seguridad de la información apoyado en una perspectiva antropológica realizado en USA, tuvo como objetivo comprender la importancia de

la seguridad de la información y el impacto del éxito que genera en una organización y como conclusión del estudio fue que existe una cohesión entre el código profesional, la conciencia de la seguridad de la información y las experiencias laborales informales, los cuales influyen sobre la cultura de seguridad de la información en una entidad. De forma similar, Santisteban et al. (2020) en el estudio sobre el análisis de las estrategias nacionales de ciberseguridad, cuyo objetivo fue analizar y diseñar Estrategias Nacionales de Ciberseguridad para mitigar ataques cibernéticos y como conclusión fue que tras el análisis de las estrategias de ciberseguridad determinaron aplicar las estrategias para combatir el cibercrimen y con ello poder ayudar a los usuarios a sensibilizarse para prevenir los ciberataques.

En relación con las definiciones la dimensión Políticas de seguridad de la Gestión de la ciberseguridad Gómez (2011) señala que se trata de declaraciones que cubren la seguridad de los sistemas, los cuales contienen definiciones y delimitaciones de responsabilidades técnicas y empresariales. Por su parte, Vega (2008) indica que la política de seguridad no solo se trata de conocer las amenazas expuestas y recursos, sino en instaurar un origen, las cuales pueden ser internas o externas. También, Dussan (2006) menciona que se considera como un instrumento que permite manejar un problema o situación con la finalidad de orientar a los miembros de una organización.

Correspondientemente al objetivo específico 3, los resultados de esta investigación en el análisis descriptivo arrojaron que la frecuencia más alta obtenida fue el grado regular en la dimensión Supervisión de actividades de la Gestión de la ciberseguridad en conjunto con el grado regular de la Concientización digital, obteniendo 80 respuestas representadas equivalentemente al 53% del total de encuestas realizadas a los usuarios administrativos de una empresa Outsourcing. A diferencia de la menor frecuencia encontrada en el grado el óptimo de la dimensión Supervisión de actividades de la Gestión de la ciberseguridad con el grado deficiente de la Concientización digital y el grado deficiente de la dimensión Evaluación de actividades de la Gestión de la ciberseguridad con el grado óptimo de la Concientización digital donde en ambos casos no se obtuvieron respuestas.

Las conclusiones estadísticas en el análisis inferencial arrojaron en la prueba de normalidad un valor de $p < 0.001$ para la dimensión tres de la variable

independiente y dependiente, por lo que demuestra que la distribución es no paramétrica. Por ende, se empleó el Rho de Spearman para resolver el grado de correlación de las variables obteniendo así un resultado de 0.818, dando un grado de correlación positiva alta y respecto al p valor < 0.001 demostrando la existencia de una significancia entre la dimensión Supervisión de actividades de la Gestión de la ciberseguridad y la concientización digital. De este modo se da por entendido la aprobación de la hipótesis nula planteada en este estudio.

En las investigaciones mencionadas con anterioridad se encuentran la de Hillman et al. (2023) en el estudio al respecto de la evaluación sobre la concientización del phishing en las empresas realizado en Israel, tuvo como objetivo examinar la efectividad de la capacitación en concientización del phishing organizacional y como conclusión demostraron que las tres oleadas simuladas de phishing obtuvieron en la primera oleada un 25%, segunda oleada 13% y tercera oleada 10% con una desviación estándar en promedio de 7.43%, por lo que demuestra que las actividades de concientización organizacional previas son efectivas. Así mismo, Rawindaran et al. (2022) en el estudio respecto al impacto de la concienciación de ciberseguridad en las PYMES usando software inteligente para combatir el ciberdelito realizado en Gales, tuvo como objetivo explorar cómo las PYMES están controlando el ciberdelito, administrando sus actividades en línea y concientizando al personal sobre ciberseguridad para una prevención de amenazas cibernéticas y como conclusión demostraron la existencia de grandes brechas en la toma de conciencia y desconocimiento del uso de software de seguridad cibernética donde se reflejó que solo un 30% entendía la terminología.. Algo similar indica Ormachea (2020) en su estudio sobre las estrategias de ciberseguridad para el reforzamiento de la seguridad, tuvo como propósito proponer tácticas integrales de ciberseguridad para el reforzamiento de la seguridad local del Perú y como conclusión determinó que la ciberseguridad es un compromiso social de la parte pública y privada, por lo que, la estrategia de Ciberseguridad del Perú es un requisito que debe ser completado.

En relación con las definiciones de la dimensión Supervisión de actividades de la Gestión de la ciberseguridad Valdivia (2014) menciona a la supervisión como un compuesto de actividades técnicas y morales que tienen la finalidad de avocarse a una mejora continua y desarrollo en una organización. Así mismo, Chiavenato

(2001) define la supervisión de actividades como una función gerencial que se implementa a nivel operativo de la empresa. El supervisor es un director que dirige las actividades de un gerente no ejecutivo, es decir, una persona que no desempeña funciones administrativas en la empresa.

Respecto a la metodología empleada en este estudio, se estableció como aplicada, ya que se desea resolver un inconveniente específico apoyándose en la búsqueda del conocimiento, además, al tener un diseño no experimental del tipo transversal correlacional solo se analiza la variable sin intervención de por medio para no alterar el origen, solo describiendo lo que se observa en un tiempo dado. Por último, dicha metodología permite desarrollar la investigación de forma adecuada entre las variables Gestión de la ciberseguridad y Concientización digital.

VI. CONCLUSIONES

Primera Correspondiendo al objetivo general, se comprueba que la Gestión de la ciberseguridad influye significativamente en la Concientización digital en los usuarios administrativos de una empresa Outsourcing, Lima 2023. Debido a que se consiguió una vinculación positiva alta y una significancia de las variables, aceptando de este modo la hipótesis planteada en esta investigación. Además, descriptivamente se concluye que el 55% de los usuarios encuestados clasifican que la Gestión de la ciberseguridad tiene una influencia regular sobre la Concientización digital.

Segunda Teniendo como objetivo específico 1, se resuelve sobre la dimensión Evaluación de riesgos de la Gestión de la ciberseguridad influye significativamente en la Concientización digital en los usuarios administrativos de una empresa Outsourcing, Lima 2023. Por motivo a que se consiguió una vinculación positiva alta y una significancia de las variables, aceptando de este modo la hipótesis planteada en esta investigación. Además, descriptivamente se concluye que el 51.7% de los usuarios encuestados clasifican que la dimensión Evaluación de riesgos de la Gestión de la ciberseguridad tiene una influencia regular sobre la Concientización digital.

Tercera Teniendo como objetivo específico 2, se establece sobre la dimensión Políticas de seguridad de la Gestión de la ciberseguridad influye significativamente en la Concientización digital en los usuarios administrativos de una empresa Outsourcing, Lima 2023. Por motivo a que se consiguió una vinculación positiva alta y una significancia de las variables, aceptando de este modo la hipótesis planteada en esta investigación. Además, descriptivamente se concluye que el 45.7% de los usuarios encuestados clasifican que la dimensión Políticas de

seguridad de la Gestión de la ciberseguridad tiene una influencia regular sobre la Concientización digital.

Cuarta Teniendo como objetivo específico 3, se dispone que la dimensión Supervisión de actividades de la Gestión de la ciberseguridad influye significativamente en la Concientización digital en los usuarios administrativos de una empresa Outsourcing, Lima 2023. Por motivo a que se consiguió una vinculación positiva alta y una significancia de las variables, aceptando de este modo la hipótesis planteada en esta investigación. Además, descriptivamente se concluye que el 53% de los usuarios encuestados clasifican que la dimensión Supervisión de actividades de la Gestión de la ciberseguridad tiene una influencia regular sobre la Concientización digital.

VII. RECOMENDACIONES

Primera Para mantener un grado elevado de vinculación entre la Gestión de la ciberseguridad con la Concientización digital en los usuarios administrativos de una empresa Outsourcing, se sugiere al Gerente General, el Gerente de Sistemas y al jefe de sistemas establecer una estrecha colaboración estratégica para implementar programas de concientización digital y fortalecer las medidas de gestión de la ciberseguridad. Además, de fomentar una cultura organizativa que priorice la seguridad y la conciencia digital para todas las áreas de la organización

Segunda Para mantener un grado elevado de vinculación entre la dimensión Evaluación de riesgos de la Gestión de la ciberseguridad con la Concientización digital en los usuarios administrativos de una empresa Outsourcing, se sugiere al Gerente de sistemas y al jefe de RRHH realizar evaluaciones periódicas de riesgos para identificar posibles vulnerabilidades y brechas en la seguridad cibernética, y utilizar estos hallazgos para desarrollar programas de concientización y acciones correctivas. Además, de integrar la evaluación de riesgos para el procesamiento en la toma de determinaciones y proyecciones estratégicas; aspectos de seguridad cibernética y conciencia digital.

Tercera Para mantener un grado elevado de vinculación entre la dimensión Políticas de seguridad de la Gestión de la ciberseguridad con la Concientización digital en los usuarios administrativos de una empresa Outsourcing, se sugiere al Gerente de sistemas y jefe de RRHH establecer una colaboración para garantizar la comunicación y difusión efectiva de las políticas de seguridad a todos los empleados, donde dichas políticas estén expresada de forma clara y concisa sobre los aspectos como el uso adecuado de la tecnología, resguardo de datos

y prevención de amenazas cibernéticas. Como también, proporcionar capacitación regular sobre las políticas de seguridad y la conciencia digital para que los usuarios comprendan y se adhieran a ellas.

Cuarta Para mantener el grado elevado de vinculación entre la dimensión Supervisión de actividades de la Gestión de la ciberseguridad con la Concientización digital en los usuarios administrativos de una empresa Outsourcing, se sugiere al Gerente de sistemas y jefe de RRHH establecer procesos de supervisión y monitoreo de actividades relacionadas a la seguridad cibernética y la conciencia digital. También, implementar herramientas y tecnologías de monitoreo de seguridad que ayuden a detectar y prevenir posibles amenazas cibernéticas, por último, realizar auditorías internas periódicamente para una evaluación efectiva de las medidas de seguridad.

REFERENCIAS

Ajzen, I. (1991). The theory of planned behavior. *Organizational Behavior and Human Decision Processes*, 50, 179-211.

Akter, S., Rajib, M., Sayib, S., Thomas, Q., Miguel, K. & Alamgir, M. (2022). Reconceptualizing cybersecurity awareness capability in the data-driven digital economy. *Ann Oper Res*. https://doi.org/10.1007/s10479-022-04844-8

Arenas, A., Ortiz, C., & Álvarez, L. (2005). Transferencia del conocimiento tecnológico al aula: Estructuración del pensamiento tecnológico mediante la enseñanza del diseño. *Revista UIS Ingenierías*, 4(2), 129-138.

Arias, J., Villasís, M., & Miranda, M. (2016). El protocolo de investigación III: la población de estudio. Revista Alergia México, 63 (2),201-206. https://www.redalyc.org/articulo.oa?id=486755023011

Baena, G. (2014). Metodología de la investigación. México, D.F.: *Grupo Editorial Patria*.

Boto-García, D. (2023). Hospitality workers' awareness and training about the risks of online crime and the occurrence of cyberattacks. *Journal of hospitality and tourism management, 55*, 240-247. https://doi.org/10.1016/j.jhtm.2023.04.010

Castillejos, B., Torres, C. & Lagunes, A. (2016). La seguridad en las competencias digitales de los millennials. *Apertura, 8*, (2). pp. 54-69. http://www.scielo.org.mx/scielo.php?script=sci_arttext&pid=S1665-61802016000300054&lng=es&tlng=es.

Chiavenato, I. (2011). Administración de recursos humanos: El capital humano de las organizaciones *(9a ed.--).* México D.F., México: McGraw - Hill.

Cienfuegos Velasco, M. A., Cienfuegos Velasco, A. (2016). Lo cuantitativo y cualitativo en la investigación. Un apoyo a su enseñanza. *Revista Iberoamericana para la Investigación y el Desarrollo Educativo, Vol. 7*, Núm. 13, 1-22. https://www.scielo.org.mx/pdf/ride/v7n13/2007-7467-ride-7-13-00015.pdf

Corletti, A. (2017) Ciberseguridad. Una estrategia Informática / Militar. *DarFE*. ISBN: 978-84-597-7205-8. https://www.ieee.es/Galerias/fichero/OtrasPublicaciones/Nacional/2018/Libro-Ciberseguridad_A.Corletti_nov2017.pd.pdf

Datt, G. & Tewari, N. (2021) A Study of Computer Users' Attitude and Awareness towards Cyber Security. *International Journal of Computer Information Systems and Industrial Management Applications. 13*. 300-307. ISSN: 21507988

De Freitas, V. (2009). Análisis y evaluación del riesgo de la información: caso de estudio Universidad Simón Bolívar. *Enlace, 6(1)*, 43-55. http://ve.scielo.org/scielo.php?script=sci_arttext&pid=S1690-75152009000100004&lng=es&tlng=es.

DGTIC, UNAM. (2014). Matriz de habilidades digitales. *UNAM.* https://educatic.unam.mx/publicaciones/matriz-habilidades-digitales-2014.pdf

Dussan, C. (2006). Políticas de seguridad informática. *Entramado, 2(1),* 86-92. ISSN: 1900-3803

Ernst & Young (2019). ¿La ciberseguridad es algo más que protección? Encuesta Global de Seguridad de la información 2018-19. *EY Building a better working world*. https://assets.ey.com/content/dam/ey-sites/ey-com/es_co/topics/corporate-social-responsibility/ey-library-la-ciberseguridad-es-algo-mas-proteccion.pdf

Fadlika, R., Ruldeviyani, Y., Butarbutar, Z., Istiqomah, R. & Fariz, A. (2023) Employee Information Security Awareness in the Power Generation Sector of PT ABC. *International Journal of Advanced Computer Science and Applications.* https://doi.org/10.14569/IJACSA.2023.0140465

Fundación Telefónica (2016) Ciberseguridad, la protección de la información en un mundo digital. *Editorial Planeta*. Madrid, España. ISBN: 978-84-08-16304-6

Galinec, D. & Luic, L. (2020). Design of conceptual model for raisingawareness of digital threats. *World Scientific and Engineering Academy and Society., 16*, 493-504. https://doi.org/ 10.37394/232015.2020.16.50

Główczyńska, K., Łyjak, G., Gruber, H., Vlková, S., Mroziewicz, D., Nagy, K., Schenk, C., & Šmerhovský, Z. (2010) Guía para la valoración de riesgos en pequeñas y medianas empresas. Evaluación del riesgo – guía de uso general. *Asociación Internacional de la Seguridad Social*. ISBN 978-3-941441-75-0

Gómez, A. (2011). Enciclopedia de la seguridad informática 2da Edición. *Editorial RA-MA. Vol. 6*. ISBN: 978-84-9964-038-5

Hernández, A., Indacochea, B., Moreno, L., Placencia, B., Quimis, A., y Ramos, M. (2018). Metodología de la Investigación Científica. *Ed. Área de Innovación y Desarrollo, S.L*. ISBN 978-8-494-82570-5

Hernández, O. (2020). Seguridad digital: conceptos y herramientas básicas. Datos Bajo llave. *Conexo*. https://conexo.org/wp-content/uploads/2020/06/Seguridad-Digital-Conceptos-y-Herramientas-B%C3%A1sicas-Mayo-2020.pdf

Hernández, R. y Mendoza, C. (2018). Metodología de la investigación. Las rutas cuantitativa, cualitativa y mixta. Ciudad de México, México: *Editorial Mc Graw Hill Education*. ISBN: 978-1-4562-6096-5

Hillman, D., Harel, Y. & Toch, E. (2023). Evaluating organizational phishing awareness training on an enterprise scale. *Computers & Security, 132*, 103364. https://doi.org/10.1016/j.cose.2023.103364

Huraj, L., Lengyelfalusy, T., Hurajová, A. & Lajčin, D. (2023). Measuring Cyber Security Awareness: A Comparison between Computer Science and Media Science Students. *TEM Journal. 12*. 623-633. ISSN 2217-8309

Karakuş, I., & Kılıç, F. (2022). Digital overview at the profiles of pre-service teachers: Digital awareness, competence and fluency. *Problems of Education in the 21st Century*, *80(2)*, 324-338. https://doi.org/10.33225/pec/22.80.324

Khan, N., Ikram, N., Murtaza, H. & Javed, M. (2023) Evaluating protection motivation-based cybersecurity awareness training on Kirkpatrick's Model. *Computers and Security, 125*, 103049. https://doi.org//10.1016/j.cose.2022.103049

Koehler, Matthew y Punya Mishra (2008), “Introducing TPCK”, en AACTE Committee on Innovation and Technology (eds.), *Handbook of Technological Pedagogical Content Knowledge (TPCK) for Educators*, Nueva York, Routledge, pp. 3-30.

Krawczyk, I., y Caputa, W. (2023). Awareness of network security and customer value – The company and customer perspective. *Technological Forecasting and Social Change, 190*, 122430. https://doi.org/10.1016/j.techfore.2023.122430

Lévano, L., Sanchez, S., Guillén, P., Tello, S., Herrera, N., y Collantes, Z. (2019). Competencias digitales y educación. Propósitos y Representaciones, 7(2), 569-588. http://dx.doi.org/10.20511/pyr2019.v7n2.329

Ley Nº 31250 (2021). Ley del Sistema Nacional de Ciencia, Tecnología e Innovación. Normas Legales N.º 16096. *Diario Oficial El Peruano*.

https://busquedas.elperuano.pe/normaslegales/ley-del-sistema-nacional-de-ciencia-tecnologia-e-innovacion-ley-n-31250-1968664-1/#:~:

Martínez, A., y Campos, W. (2015). Correlación entre Actividades de Interacción Social Registradas con Nuevas Tecnologías y el grado de Aislamiento Social en los Adultos Mayores. *Revista mexicana de ingeniería biomédica*, *36(3),* 181-191. https://doi.org/10.17488/RMIB.36.3.4

Mendivil, J., Sanz, B. & Gutierrez, M. (2022). Competency-based cybersecurity training and awareness: a systematic literature review. *Pixel-Bit: Revista de Medios y Educación., 63*, 197–225. https://doi.org/10.12795/PIXELBIT.91640

Morduchowicz, R. (2021). Competencias y habilidades digitales. Organización de las Naciones Unidas para la Educación, la Ciencia y la Cultura y la Oficina Regional de Ciencias de la UNESCO. *UNESCO*. https://unesdoc.unesco.org/in/documentViewer.xhtml?v=2.1.196&id=p::usmarcdef_0000380113&file=/in/rest/annotationSVC/DownloadWatermarkedAttachment/attach_import_3a95803f-8657-466e-9723-130de6e7f32d%3F_%3D380113spa.pdf&locale=en&multi=true&ark=/ark:/48223/pf0000380113/PDF/380113spa.pdf#%5B%7B%22num%22%3A50%2C%22gen%22%3A0%7D%2C%7B%22name%22%3A%22XYZ%22%7D%2C-1%2C839%2C0%5D

Moreno, J. (2008). Defensa en profundidad. *Universidad Piloto de Colombia.* http://polux.unipiloto.edu.co:8080/00001345.pdf

Nwankpa, J. K., y Datta, P. (2023). Remote Vigilance: The Roles of Cyber Awareness and Cybersecurity Policies Among Remote Workers. *Computers & Security*, 103266. https://doi.org/10.1016/j.cose.2023.103266

Ñaupas, H., Valdivia, M., Palacios, J. y Romero, H. (2018). Metodología de la investigación cuantitativa-cualitativa y redacción de la tesis. *Ed. Ediciones de la U*. ISBN 978-958-762-876-0.

Ormachea, J. (2020) Estrategias integradas de ciberseguridad para el fortalecimiento de la seguridad nacional. *Revista de Ciencia e Investigación en Degesna-CAEN. 1*, 36-48. ISSN: 2709-1422

Pinzón, I. (2014). Gestión del riesgo en Seguridad Informática. *Universidad Piloto de Colombia.* http://repository.unipiloto.edu.co/bitstream/handle/20.500.12277/2840/Gestion%20del%20riesgo%20en%20seguridad%20informatica.pdf?sequence=1&%3BisAllowed=y

PRONABEC (09 de julio de 2021). Plan de Concientización y Sensibilización en Seguridad de la Información. *Ministerio de Educación*. http://www.pronabec.gob.pe/SGSI/PLAN.SGSI.02-PRONABEC_Plan%20de%20Concientizacion%20y%20Sensibilizacion.pdf

Rawindaran, N., Jayal, A. y Prakash, E. (2022). Exploration of the Impact of Cybersecurity Awareness on Small and Medium Enterprises (SMEs) in Wales Using Intelligent Software to Combat Cybercrime. *MDPI*, 11 (12). https://doi.org/10.3390/computers11120174

Reeves, A., Calic, D., y Delfabbro, P. (2023). “Generic and unusable”1: Understanding employee perceptions of cybersecurity training and measuring advice fatigue. *Computers & Security, 128*, 103137. https://doi.org/10.1016/j.cose.2023.103137

Resolución de la fiscalía de la Nación. Sistema de Gestión de Seguridad de la Información y Ciberseguridad (SGSI-C). 22 de febrero del 2021. Nº 246-2021-MP-FN.

Rodríguez, G. (2020). *Análisis comparativo de los modelos Defensa en Profundidad y MSPI, para la implementación de la Seguridad Informática en el sector privado del país.* Universidad Nacional Abierta y a Distancia. Bogotá D.C. Colombia.

Ruiz, C. (2013). Instrumentos y técnicas de investigación educativa (3.a ed.). *DANAGA Training and Consulting*.

Sánchez, H., Reyes, C. y Mejía K. (2018). Manual de términos en investigación científica, tecnológica y humanística. (1era ed.). Lima, Perú: *Editorial Universidad Ricardo Palma*. ISBN 978-612-47351-4-1

Santisteban, A., Cunyarachi, L. & Andrade, L. (2020) Analysis of national cybersecurity strategies. *International Journal of Advanced Computer Science and Applications, 11, 12.* ISSN: 2158107X

Seyal, A. y Mohd, A. (2017). Theory of Planned Behavior: New Research. New York, United States: *Editorial Nova Science Publishers*, Inc. ISBN: 9781536113105

Tejay, G. y Mohammed, Z. (2023). Cultivating security culture for information security success: A mixed-methods study based on anthropological perspective. *Information & Management*. *60*. 103751. https://doi.org/10.1016/j.im.2022.103751

Valdivia, E. (2014). *La supervisión como actividad primordial en el desarrollo profesional del IQI*. Instituto Politécnico Nacional. https://tesis.ipn.mx/bitstream/handle/123456789/17310/25-1-16716.pdf?sequence=1&isAllowed=y

Vega Velasco, Walter. (2008). Políticas y seguridad de la información. *Fides et Ratio - Revista de Difusión cultural y científica de la Universidad La Salle en Bolivia*, 2(2), 63-69. http://www.scielo.org.bo/scielo.php?script=sci_arttext&pid=S2071-081X2008000100008&lng=es&tlng=es.

Verizon (2022). DBIR 2022 Data Breach Investigations Report. *Verizon Communications Inc (VZ)*. https://www.verizon.com/business/resources/reports/dbir/

Vidal, R., Alcober, J., Cervelló, C., Fernández, T., Garcia, E. & Yúfera, J. (2021) Creating Digital Awareness. *Network Engineering Department Universitat Politecnica de Catalunya (UPC).* https://upcommons.upc.edu/bitstream/handle/2117/355753/Article_JITEL21-ENTEL-EETAC-UPC.pdf;jsessionid=1F05EE7E010680FA3F69A30EFA0CF73C?sequence=1

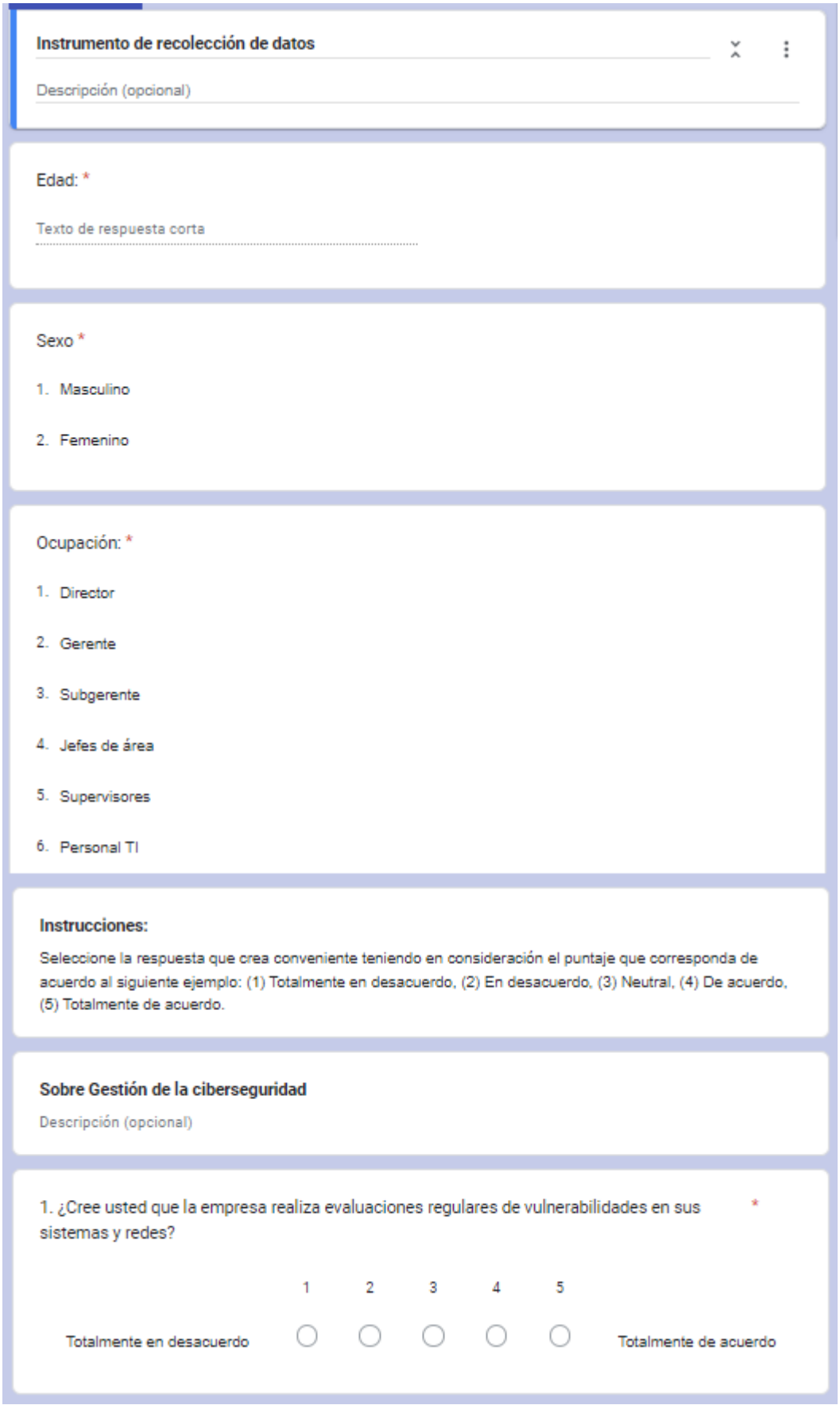
ANEXOS

Anexo 1: Tabla de operacionalización de variables

Variable de estudio	Definición conceptual	Definición operacional	Dimensión	Indicadores	Escala de medición
Variable 1: Gestión de la ciberseguridad	Resolución peruana SBS (2021) menciona a la gestión de la seguridad de la información y ciberseguridad (SGSI-C) como una lista de reglas, procedimientos, técnicas, funciones y actividades diseñadas para identificar y resguardar los activos de información, identificar incidentes de seguridad, predecir respuestas y recuperarse de incidentes de ciberseguridad	Se operacionalizó mediante 3 dimensiones: evaluación de riesgos, políticas de seguridad y supervisión de actividades; estas dimensiones serán medidas en un cuestionario.	Evaluación de riesgos	Exposición Detección	Se usará un cuestionario de escala ordinal de Likert Totalmente en desacuerdo (1), En desacuerdo (2), Neutral (3), De acuerdo (4), Totalmente de acuerdo (5).
			Políticas de seguridad	Control Documentación	
			Supervisión de actividades	Monitoreo Análisis	
Variable 2: Concientización digital	Según Karakuş y Kılıç (2022) indican que la conciencia digital es una capacidad de conocer, apreciar y observar el entorno que rodea al individuo en afinidad al campo de las tecnologías digitales.	Se operacionalizó mediante 3 dimensiones: conocimiento tecnológico, habilidad digital y seguridad digital; estas dimensiones serán medidas en un cuestionario.	Conocimiento tecnológico	Comprensión Usabilidad	
			Habilidad digital	Competencia Evaluación	
			Seguridad digital	Protección Prevención	

Anexo 2: Instrumento de recolección de datos

Formulario en Google



Instrumento de recolección de datos

Descripción (opcional)

Edad: *

Texto de respuesta corta

Sexo *

1. Masculino
2. Femenino

Ocupación: *

1. Director
2. Gerente
3. Subgerente
4. Jefes de área
5. Supervisores
6. Personal TI

Instrucciones:

Seleccione la respuesta que crea conveniente teniendo en consideración el puntaje que corresponda de acuerdo al siguiente ejemplo: (1) Totalmente en desacuerdo, (2) En desacuerdo, (3) Neutral, (4) De acuerdo, (5) Totalmente de acuerdo.

Sobre Gestión de la ciberseguridad

Descripción (opcional)

1. ¿Cree usted que la empresa realiza evaluaciones regulares de vulnerabilidades en sus sistemas y redes? *

	1	2	3	4	5	
Totalmente en desacuerdo	○	○	○	○	○	Totalmente de acuerdo

2. ¿Cree usted que la empresa implementa medidas proactivas para mitigar las vulnerabilidades? *

	1	2	3	4	5	
Totalmente en desacuerdo	○	○	○	○	○	Totalmente de acuerdo

3. ¿Cree usted que la empresa tiene sistemas de detección de intrusiones en tiempo real? *

	1	2	3	4	5	
Totalmente en desacuerdo	○	○	○	○	○	Totalmente de acuerdo

4. ¿Cree usted que la empresa cuenta con un plan de respuesta a incidentes? *

	1	2	3	4	5	
Totalmente en desacuerdo	○	○	○	○	○	Totalmente de acuerdo

5. ¿Considera usted que las políticas de seguridad establecen claramente los controles y medidas necesarios para proteger la información? *

	1	2	3	4	5	
Totalmente en desacuerdo	○	○	○	○	○	Totalmente de acuerdo

6. ¿Considera usted que la empresa cuenta con mecanismos de supervisión y control para las políticas de seguridad? *

	1	2	3	4	5	
Totalmente en desacuerdo	○	○	○	○	○	Totalmente de acuerdo

7. ¿Considera usted que las políticas de seguridad son revisadas y validadas para garantizar un correcto estándar de seguridad? *

	1	2	3	4	5	
Totalmente en desacuerdo	○	○	○	○	○	Totalmente de acuerdo

8. ¿Considera usted que la documentación de la gestión de ciberseguridad está actualizada y accesible al personal? *

	1	2	3	4	5	
Totalmente en desacuerdo	○	○	○	○	○	Totalmente de acuerdo

9. ¿Cree usted que la empresa cuenta con sistemas y herramientas de monitoreo en tiempo real que detectan y alertan sobre actividades sospechosas en la red y sistemas? *

	1	2	3	4	5	
Totalmente en desacuerdo	○	○	○	○	○	Totalmente de acuerdo

10. ¿Cree usted que existen protocolos y procedimientos de respuesta identificados para el monitoreo de actividades? *

	1	2	3	4	5	
Totalmente en desacuerdo	○	○	○	○	○	Totalmente de acuerdo

11. ¿Cree usted que la empresa realiza análisis periódicos de los registros para identificar patrones y tendencias para mejorar la seguridad? *

	1	2	3	4	5	
Totalmente en desacuerdo	○	○	○	○	○	Totalmente de acuerdo

12. ¿Cree usted que la empresa realice análisis forense para la toma de medidas correctivas? *

	1	2	3	4	5	
Totalmente en desacuerdo	○	○	○	○	○	Totalmente de acuerdo

Sobre Concientización digital

Descripción (opcional)

13. ¿Considera usted que cuenta con un conocimiento básicos de la tecnología y cómo funcionan los dispositivos y aplicaciones digitales? *

	1	2	3	4	5	
Totalmente en desacuerdo	○	○	○	○	○	Totalmente de acuerdo

14. ¿Considera usted que entiende sobre los riesgos que conlleva las tecnologías digitales, como la privacidad, phishing y malware? *

	1	2	3	4	5	
Totalmente en desacuerdo	○	○	○	○	○	Totalmente de acuerdo

15. ¿Considera usted que las herramientas y servicios digitales son intuitivos y están diseñados teniendo en cuenta las necesidades del usuario? *

	1	2	3	4	5	
Totalmente en desacuerdo	○	○	○	○	○	Totalmente de acuerdo

16. ¿Considera usted que el acceso a la información y los servicios en línea son convenientes y permiten agilizar actividades? *

	1	2	3	4	5	
Totalmente en desacuerdo	○	○	○	○	○	Totalmente de acuerdo

17. ¿Considera usted que cuenta con habilidades suficientes para utilizar una variedad de aplicaciones y herramientas digitales para realizar tareas y actividades en línea? *

	1	2	3	4	5	
Totalmente en desacuerdo	○	○	○	○	○	Totalmente de acuerdo

18. ¿Considera usted que cuenta con la capacidad de evaluar críticamente la calidad y la veracidad de la información encontrada en Internet? *

	1	2	3	4	5	
Totalmente en desacuerdo	○	○	○	○	○	Totalmente de acuerdo

19. ¿Considera usted que cuenta con la capacidad de proteger su privacidad y seguridad en línea mediante el uso de configuraciones de privacidad y medidas de seguridad digital? *

	1	2	3	4	5	
Totalmente en desacuerdo	○	○	○	○	○	Totalmente de acuerdo

20. ¿Considera usted que puede utilizar de manera efectiva las herramientas y recursos para su protección y seguridad digital, como antivirus y contraseñas seguras? *

	1	2	3	4	5	
Totalmente en desacuerdo	○	○	○	○	○	Totalmente de acuerdo

21. ¿Cree usted que cuenta con la capacidad de identificar y evitar las principales amenazas en línea, como el phishing y el malware? *

	1	2	3	4	5	
Totalmente en desacuerdo	○	○	○	○	○	Totalmente de acuerdo

22. ¿Cree usted que es consciente sobre los riesgos asociados con la divulgación de información personal en línea? *

	1	2	3	4	5	
Totalmente en desacuerdo	○	○	○	○	○	Totalmente de acuerdo

23. ¿Cree usted que puede reconocer y evitar comportamientos de riesgo en línea, como descargar archivos adjuntos sospechosos o hacer clic en enlaces no confiables? *

	1	2	3	4	5	
Totalmente en desacuerdo	○	○	○	○	○	Totalmente de acuerdo

24. ¿Cree usted que es importante mantener sus dispositivos y aplicaciones actualizados con las últimas actualizaciones de seguridad? *

	1	2	3	4	5	
Totalmente en desacuerdo	○	○	○	○	○	Totalmente de acuerdo

Anexo 3: Modelo de consentimiento informado

Formulario en Google

Modelo de consentimiento informado

Título de la investigación: Gestión de la ciberseguridad y concientización digital en los usuarios administrativos de una empresa Outsourcing, Lima 2023.

Investigador: Angeles Gonzales, Edwin Ivan.

Propósito del estudio

Le invitamos a participar en la investigación titulada "Gestión de la ciberseguridad y concientización digital en los usuarios administrativos de una empresa Outsourcing, Lima 2023", cuyo objetivo es determinar la influencia de la gestión de la ciberseguridad en la concientización digital en los usuarios administrativos de una empresa Outsourcing, Lima 2023. Esta investigación es desarrollada por estudiantes de posgrado de la Maestría en Ingeniería de Sistemas con mención en Tecnologías de la Información, de la Universidad César Vallejo del campus Lima - Norte, aprobado por la autoridad correspondiente de la Universidad y con el permiso de la institución Universidad César Vallejo.

Describir el impacto del problema de la investigación.

¿De qué manera influye la gestión de la ciberseguridad en la concientización digital en los usuarios administrativos de una empresa Outsourcing, Lima 2023?

Procedimiento

Si usted decide participar en la investigación se realizará lo siguiente (enumerar los procedimientos del estudio):

1. Se realizará una encuesta o entrevista donde se recogerán datos personales y algunas preguntas sobre la investigación titulada: Gestión de la ciberseguridad y concientización digital en los usuarios administrativos de una empresa Outsourcing, Lima 2023".

2. Esta encuesta o entrevista tendrá un tiempo aproximado de 15 minutos y se realizará en el ambiente vía web. Las respuestas al cuestionario o guía de entrevista serán codificadas usando un número de identificación y, por lo tanto, serán anónimas.

Participación voluntaria (principio de autonomía):

Puede hacer todas las preguntas para aclarar sus dudas antes de decidir si desea participar o no, y su decisión será respetada. Posterior a la aceptación no desea continuar puede hacerlo sin ningún problema.

Riesgo (principio de No maleficencia):

Indicar al participante la existencia que NO existe riesgo o daño al participar en la investigación. Sin embargo, en el caso que existan preguntas que le puedan generar incomodidad. Usted tiene la libertad de responderlas o no.

Beneficios (principio de beneficencia):

Se le informará que los resultados de la investigación se le alcanzará a la institución al término de la investigación. No recibirá ningún beneficio económico ni de ninguna otra índole. El estudio no va a aportar a la salud individual de la persona, sin embargo, los resultados del estudio podrán convertirse en beneficio de la salud pública.

Confidencialidad (principio de justicia):

Los datos recolectados deben ser anónimos y no tener ninguna forma de identificar al participante. Garantizamos que la información que usted nos brinde es totalmente Confidencial y no será usada para ningún otro propósito fuera de la investigación. Los datos permanecerán bajo custodia del investigador principal y pasado un tiempo determinado serán eliminados convenientemente.

Problemas o preguntas:

Si tiene preguntas sobre la investigación puede contactar con el Investigador: Angeles Gonzales, Edwin Ivan email: eangelesgo10@ucvvirtual.edu.pe y Docente asesor: Poletti Gaitan, Eduardo Humberto email: epolettig@ucvvirtual.edu.pe

Consentimiento

Después de haber leído los propósitos de la investigación autorizo participar en la investigación antes mencionada.

Nombre y apellidos: *

Texto de respuesta corta

Correo electrónico

Texto de respuesta corta

Fecha y hora: *

Mes, día, año

Hora

Anexo 4: Evaluación por juicio de expertos

Primera evaluación

Respetado juez: Usted ha sido seleccionado para evaluar el instrumento "Cuestionario para usuarios administrativos de una empresa Outsourcing". La evaluación del instrumento es de gran relevancia para lograr que sea válido y que los resultados obtenidos a partir de éste sean utilizados eficientemente; aportando al quehacer psicológico. Agradecemos su valiosa colaboración.

1. Datos generales del juez

Nombre del juez:	Marlon Acuña Benites	
Grado profesional:	Maestría ( )	Doctor (X)
Área de formación académica:	Clínica ( ) Educativa (X)	Social ( ) Organizacional ( )
Áreas de experiencia profesional:	Docente / Investigador	
Institución donde labora:	Universidad César Vallejo	
Tiempo de experiencia profesional en el área:	2 a 4 años ( ) Más de 5 años (x)	
Experiencia en Investigación Psicométrica: (si corresponde)		

2. Propósito de la evaluación:

Validar el contenido del instrumento, por juicio de expertos.

3. Datos de la escala (Colocar nombre de la escala, cuestionario o inventario)

Nombre de la Prueba:	Cuestionario para usuarios administrativos de una empresa Outsourcing
Autor:	Angeles Gonzales, Edwin Ivan
Procedencia:	Universidad César Vallejo
Administración:	Formularios de Google
Tiempo de aplicación:	15 minutos
Ámbito de aplicación:	24 ítems: V.D. (12 ítems) y V.I. (12 ítems)
Significación:	Explicar Cómo está compuesta la escala (dimensiones, áreas, ítems por área, explicación breve de cuál es el objetivo de medición)

4. Soporte teórico

Escala / ÁREA	Subescala (dimensiones)	Definición
Gestión de la ciberseguridad	Evaluación de riesgos	Señala que es un proceso de identificación, análisis y valoración donde permite establecer un grado de amenaza y riesgo asociado teniendo en consideración el resultado del proceso y la identificación de los controles adecuados. (Pinzón, 2014).
	Políticas de seguridad	Señala que se trata de declaraciones que cubre la seguridad de los sistemas, los cuales contienen definiciones y delimitaciones de responsabilidades técnicas y empresariales. (Gómez, 2011)
	Supervisión de actividades	Define como una función gerencial que se implementa a nivel operativo de la empresa. El supervisor es un director que dirige las actividades de un gerente no ejecutivo, es decir, una persona que no desempeña funciones administrativas en la empresa. (Chiavenato, 2001)
Concientización digital	Conocimiento tecnológico	Menciona que el conocimiento tecnológico hace referencia a todo tipo de conocimiento tecnológico que no solo abarque temas de informática, sino que va más del campo. (Koehler y Mishra, 2008)
	Habilidad digital	Indica que se trata de un conglomerado de conocimientos, portes, artes, condiciones y destrezas que se necesitan para usar las tecnologías. (Morduchowicz, 2021)
	Seguridad digital	Menciona a la seguridad digital como un compuesto de acciones que sirven para proteger y controlar las comunicaciones, información y datos siempre con la premisa de la triada sobre seguridad de la información. (Hernández, 2022)

5. Presentación de instrucciones para el juez:

A continuación, a usted le presento el cuestionario para usuarios administrativos de una empresa Outsourcing elaborado por Angeles Gonzales Edwin Ivan en el año 2023. De acuerdo con los siguientes indicadores califique cada uno de los ítems según corresponda.

Categoría	Calificación	Indicador
CLARIDAD El ítem se comprende fácilmente, es decir, su sintáctica y semántica son adecuadas.	1. No cumple con el criterio	El ítem no es claro.
	2. Bajo Nivel	El ítem requiere bastantes modificaciones o una modificación muy grande en el uso de las palabras de acuerdo con su significado o por la ordenación de estas.
	3. Moderado nivel	Se requiere una modificación muy específica de algunos de los términos del ítem.
	4. Alto nivel	El ítem es claro, tiene semántica y sintaxis adecuada.
COHERENCIA El ítem tiene relación lógica con la dimensión o indicador que está midiendo.	1. totalmente en desacuerdo (no cumple con el criterio)	El ítem no tiene relación lógica con la dimensión.
	2. Desacuerdo (bajo nivel de acuerdo)	El ítem tiene una relación tangencial /lejana con la dimensión.
	3. Acuerdo (moderado nivel)	El ítem tiene una relación moderada con la dimensión que se está midiendo.
	4. Totalmente de Acuerdo (alto nivel)	El ítem se encuentra está relacionado con la dimensión que está midiendo.
RELEVANCIA El ítem es esencial o importante, es decir debe ser incluido.	1. No cumple con el criterio	El ítem puede ser eliminado sin que se vea afectada la medición de la dimensión.
	2. Bajo Nivel	El ítem tiene alguna relevancia, pero otro ítem puede estar incluyendo lo que mide éste.
	3. Moderado nivel	El ítem es relativamente importante.
	4. Alto nivel	El ítem es muy relevante y debe ser incluido.

Leer con detenimiento los ítems y calificar en una escala de 1 a 4 su valoración, así como solicitamos brinde sus observaciones que considere pertinente

1 No cumple con el criterio
2. Bajo Nivel
3. Moderado nivel
4. Alto nivel

Variable Independiente: Gestión de la ciberseguridad

Dimensiones del instrumento:

- Primera dimensión: Evaluación de riesgos
- Objetivos de la Dimensión: Identificar el cumplimiento de la evaluación de riesgos en la empresa Outsourcing.

Indicadores	Ítem	Claridad	Coherencia	Relevancia	Observaciones / Recomendaciones
Exposición	¿Cree usted que la empresa realiza evaluaciones regulares de vulnerabilidades en sus sistemas y redes?	4	4	4	APLICABLE
Exposición	¿Cree usted que la empresa implementa medidas proactivas para mitigar las vulnerabilidades?	4	4	4	APLICABLE
Detección	¿Cree usted que la empresa tiene sistemas de detección de intrusiones en tiempo real?	4	4	4	APLICABLE
Detección	¿Cree usted que la empresa cuenta con un plan de respuesta a incidentes?	4	4	4	APLICABLE

- Segunda dimensión: Políticas de seguridad
- Objetivos de la Dimensión: Identificar la aplicación de las políticas de seguridad en la empresa Outsourcing.

Indicadores	Ítem	Claridad	Coherencia	Relevancia	Observaciones / Recomendaciones
Control	¿Considera usted que las políticas de seguridad establecen claramente los controles y medidas necesarios para proteger la información?	4	4	4	APLICABLE
Control	¿Considera usted que la empresa cuenta con mecanismos de supervisión y control para las políticas de seguridad?	4	4	4	APLICABLE
Documentación	¿Considera usted que las políticas de seguridad son revisadas y validadas para garantizar un correcto estándar de seguridad?	4	4	4	APLICABLE

Indicadores	Ítem	Claridad	Coherencia	Relevancia	Observaciones / Recomendaciones
Documentación	¿Considera usted que la documentación de la gestión de ciberseguridad está actualizada y accesible al personal?	4	4	4	APLICABLE

- Tercera dimensión: Supervisión de actividades
- Objetivos de la Dimensión: Identificar la aplicación de actividades de monitoreo en la empresa Outsourcing.

Indicadores	Ítem	Claridad	Coherencia	Relevancia	Observaciones / Recomendaciones
Monitoreo	¿Cree usted que la empresa cuenta con sistemas y herramientas de monitoreo en tiempo real que detectan y alertan sobre actividades sospechosas en la red y sistemas?	4	4	4	APLICABLE
Monitoreo	¿Cree usted que existen protocolos y procedimientos de respuesta identificados para el monitoreo de actividades?	4	4	4	APLICABLE
Análisis	¿Cree usted que la empresa realiza análisis periódicos de los registros para identificar patrones y tendencias para mejorar la seguridad?	4	4	4	APLICABLE
Análisis	¿Cree usted que la empresa realice análisis forense para la toma de medidas correctivas?	4	4	4	APLICABLE

Variable Dependiente: Concientización digital

Dimensiones del instrumento:

- Primera dimensión: Conocimiento tecnológico
- Objetivos de la Dimensión: Identificar el nivel de conocimiento y el uso que tienen los usuarios respecto a la tecnología.

Indicadores	Ítem	Claridad	Coherencia	Relevancia	Observaciones / Recomendaciones
Comprensión	¿Considera usted que cuenta con un conocimiento básicos de la tecnología y cómo funcionan los dispositivos y aplicaciones digitales?	4	4	4	APLICABLE

Indicadores	Ítem	Claridad	Coherencia	Relevancia	Observaciones / Recomendaciones
Comprensión	¿Considera usted que entiende sobre los riesgos que conlleva las tecnologías digitales, como la privacidad, phishing y malware?	4	4	4	APLICABLE
Usabilidad	¿Considera usted que las herramientas y servicios digitales son intuitivos y están diseñados teniendo en cuenta las necesidades del usuario?	4	4	4	APLICABLE
Usabilidad	¿Considera usted que el acceso a la información y los servicios en línea son convenientes y permiten agilizar actividades?	4	4	4	APLICABLE

- Segunda dimensión: Habilidad digital
- Objetivos de la Dimensión: Identificar la competencia y grado del usuario en los entornos digitales.

Indicadores	Ítem	Claridad	Coherencia	Relevancia	Observaciones / Recomendaciones
Competencia	¿Considera usted que cuenta con habilidades suficientes para utilizar una variedad de aplicaciones y herramientas digitales para realizar tareas y actividades en línea?	4	4	4	APLICABLE
Competencia	¿Considera usted que cuenta con la capacidad de evaluar críticamente la calidad y la veracidad de la información encontrada en Internet?	4	4	4	APLICABLE
Evaluación	¿Considera usted que cuenta con la capacidad de proteger su privacidad y seguridad en línea mediante el uso de configuraciones de privacidad y medidas de seguridad digital?	4	4	4	APLICABLE
Evaluación	¿Considera usted que puede utilizar de manera efectiva las herramientas y recursos para su protección y seguridad digital, como antivirus y contraseñas seguras?	4	4	4	APLICABLE

- Tercera dimensión: Seguridad digital
- Objetivos de la Dimensión: Identificar el nivel de protección y prevención del usuario frente a las actividades en línea.

Indicadores	Ítem	Claridad	Coherencia	Relevancia	Observaciones / Recomendaciones
Protección	¿Cree usted que cuenta con la capacidad de identificar y evitar las principales amenazas en línea, como el phishing y el malware?	4	4	4	APLICABLE
Protección	¿Cree usted que es consciente sobre los riesgos asociados con la divulgación de información personal en línea?	4	4	4	APLICABLE
Prevención	¿Cree usted que puede reconocer y evitar comportamientos de riesgo en línea, como descargar archivos adjuntos sospechosos o hacer clic en enlaces no confiables?	4	4	4	APLICABLE
Prevención	¿Cree usted que es importante mantener sus dispositivos y aplicaciones actualizados con las últimas actualizaciones de seguridad?	4	4	4	APLICABLE

Dr. Marlon Acuña Benites
DNI: 42097456
Ing. de Sistemas / Investigador

Pd.: el presente formato debe tomar en cuenta:
Williams y Webb (1994) así como Powell (2003), mencionan que no existe un consenso respecto al número de expertos a emplear. Por otra parte, el número de jueces que se debe emplear en un juicio depende del nivel de experticia y de la diversidad del conocimiento. Así, mientras Gable y Wolf (1993), Grant y Davis (1997), y Lynn (1986) (citados en McGartland et al. 2003) sugieren un rango de **2** hasta **20 expertos**, Hyrkäs et al. (2003) manifiestan que **10 expertos** brindarán una estimación confiable de la validez de contenido de un instrumento (cantidad mínimamente recomendable para construcciones de nuevos instrumentos). Si un 80 % de los expertos han estado de acuerdo con la validez de un ítem éste puede ser incorporado al instrumento (Voutilainen & Liukkonen, 1995, citados en Hyrkäs et al. (2003).
Ver : https://www.revistaespacios.com/cited2017/cited2017-23.pdf entre otra bibliografía.

Segunda evaluación

Respetado juez: Usted ha sido seleccionado para evaluar el instrumento "Cuestionario para usuarios administrativos de una empresa Outsourcing". La evaluación del instrumento es de gran relevancia para lograr que sea válido y que los resultados obtenidos a partir de éste sean utilizados eficientemente; aportando al quehacer psicológico. Agradecemos su valiosa colaboración.

1. Datos generales del juez

Nombre del juez:	Alindor Fernando Espinoza Espinoza
Grado profesional:	Maestría ( ) Doctor (X)
Área de formación académica:	Clínica ( ) Social ( ) Educativa (X) Organizacional ( )
Áreas de experiencia profesional:	Docente / Investigador
Institución donde labora:	Universidad César Vallejo
Tiempo de experiencia profesional en el área:	2 a 4 años ( ) Más de 5 años (x)
Experiencia en Investigación Psicométrica: (si corresponde)	

2. Propósito de la evaluación:

Validar el contenido del instrumento, por juicio de expertos.

3. Datos de la escala (Colocar nombre de la escala, cuestionario o inventario)

Nombre de la Prueba:	Cuestionario para usuarios administrativos de una empresa Outsourcing
Autor:	Angeles Gonzales, Edwin Ivan
Procedencia:	Universidad César Vallejo
Administración:	Formularios de Google
Tiempo de aplicación:	15 minutos
Ámbito de aplicación:	24 ítems: V.D. (12 ítems) y V.I. (12 ítems)
Significación:	Explicar Cómo está compuesta la escala (dimensiones, áreas, ítems por área, explicación breve de cuál es el objetivo de medición)

4. Soporte teórico

Escala / ÁREA	Subescala (dimensiones)	Definición
Gestión de la ciberseguridad	Evaluación de riesgos	Señala que es un proceso de identificación, análisis y valoración donde permite establecer un grado de amenaza y riesgo asociado teniendo en consideración el resultado del proceso y la identificación de los controles adecuados. (Pinzón, 2014).
	Políticas de seguridad	Señala que se trata de declaraciones que cubre la seguridad de los sistemas, los cuales contienen definiciones y delimitaciones de responsabilidades técnicas y empresariales. (Gómez, 2011)
	Supervisión de actividades	Define como una función gerencial que se implementa a nivel operativo de la empresa. El supervisor es un director que dirige las actividades de un gerente no ejecutivo, es decir, una persona que no desempeña funciones administrativas en la empresa. (Chiavenato, 2001)
Concientización digital	Conocimiento tecnológico	Menciona que el conocimiento tecnológico hace referencia a todo tipo de conocimiento tecnológico que no solo abarque temas de informática, sino que va más del campo. (Koehler y Mishra, 2008)
	Habilidad digital	Indica que se trata de un conglomerado de conocimientos, portes, artes, condiciones y destrezas que se necesitan para usar las tecnologías. (Morduchowicz, 2021)
	Seguridad digital	Menciona a la seguridad digital como un compuesto de acciones que sirven para proteger y controlar las comunicaciones, información y datos siempre con la premisa de la triada sobre seguridad de la información. (Hernández, 2022)

5. Presentación de instrucciones para el juez:

A continuación, a usted le presento el cuestionario para usuarios administrativos de una empresa Outsourcing elaborado por Angeles Gonzales Edwin Ivan en el año 2023. De acuerdo con los siguientes indicadores califique cada uno de los ítems según corresponda.

Categoría	Calificación	Indicador
CLARIDAD El ítem se comprende fácilmente, es decir, su sintáctica y semántica son adecuadas.	1. No cumple con el criterio	El ítem no es claro.
	2. Bajo Nivel	El ítem requiere bastantes modificaciones o una modificación muy grande en el uso de las palabras de acuerdo con su significado o por la ordenación de estas.
	3. Moderado nivel	Se requiere una modificación muy específica de algunos de los términos del ítem.
	4. Alto nivel	El ítem es claro, tiene semántica y sintaxis adecuada.
COHERENCIA El ítem tiene relación lógica con la dimensión o indicador que está midiendo.	1. totalmente en desacuerdo (no cumple con el criterio)	El ítem no tiene relación lógica con la dimensión.
	2. Desacuerdo (bajo nivel de acuerdo)	El ítem tiene una relación tangencial /lejana con la dimensión.
	3. Acuerdo (moderado nivel)	El ítem tiene una relación moderada con la dimensión que se está midiendo.
	4. Totalmente de Acuerdo (alto nivel)	El ítem se encuentra está relacionado con la dimensión que está midiendo.
RELEVANCIA El ítem es esencial o importante, es decir debe ser incluido.	1. No cumple con el criterio	El ítem puede ser eliminado sin que se vea afectada la medición de la dimensión.
	2. Bajo Nivel	El ítem tiene alguna relevancia, pero otro ítem puede estar incluyendo lo que mide éste.
	3. Moderado nivel	El ítem es relativamente importante.
	4. Alto nivel	El ítem es muy relevante y debe ser incluido.

Leer con detenimiento los ítems y calificar en una escala de 1 a 4 su valoración, así como solicitamos brindesus observaciones que considere pertinente

1 No cumple con el criterio
2. Bajo Nivel
3. Moderado nivel
4. Alto nivel

Variable Independiente: Gestión de la ciberseguridad

Dimensiones del instrumento:

- Primera dimensión: Evaluación de riesgos
- Objetivos de la Dimensión: Identificar el cumplimiento de la evaluación de riesgos en la empresa Outsourcing.

Indicadores	Ítem	Claridad	Coherencia	Relevancia	Observaciones / Recomendaciones
Exposición	¿Cree usted que la empresa realiza evaluaciones regulares de vulnerabilidades en sus sistemas y redes?	4	4	4	APLICABLE
Exposición	¿Cree usted que la empresa implementa medidas proactivas para mitigar las vulnerabilidades?	4	4	3	APLICABLE
Detección	¿Cree usted que la empresa tiene sistemas de detección de intrusiones en tiempo real?	4	4	4	APLICABLE
Detección	¿Cree usted que la empresa cuenta con un plan de respuesta a incidentes?	4	4	4	APLICABLE

- Segunda dimensión: Políticas de seguridad
- Objetivos de la Dimensión: Identificar la aplicación de las políticas de seguridad en la empresa Outsourcing.

Indicadores	Ítem	Claridad	Coherencia	Relevancia	Observaciones / Recomendaciones
Control	¿Considera usted que las políticas de seguridad establecen claramente los controles y medidas necesarios para proteger la información?	4	4	4	APLICABLE
Control	¿Considera usted que la empresa cuenta con mecanismos de supervisión y control para las políticas de seguridad?	3	4	4	APLICABLE
Documentación	¿Considera usted que las políticas de seguridad son revisadas y validadas para garantizar un correcto estándar de seguridad?	3	3	3	APLICABLE

Indicadores	Ítem	Claridad	Coherencia	Relevancia	Observaciones / Recomendaciones
Documentación	¿Considera usted que la documentación de la gestión de ciberseguridad está actualizada y accesible al personal?	4	4	4	APLICABLE

- Tercera dimensión: Supervisión de actividades
- Objetivos de la Dimensión: Identificar la aplicación de actividades de monitoreo en la empresa Outsourcing.

Indicadores	Ítem	Claridad	Coherencia	Relevancia	Observaciones / Recomendaciones
Monitoreo	¿Cree usted que la empresa cuenta con sistemas y herramientas de monitoreo en tiempo real que detectan y alertan sobre actividades sospechosas en la red y sistemas?	3	3	3	APLICABLE
Monitoreo	¿Cree usted que existen protocolos y procedimientos de respuesta identificados para el monitoreo de actividades?	4	4	4	APLICABLE
Análisis	¿Cree usted que la empresa realiza análisis periódicos de los registros para identificar patrones y tendencias para mejorar la seguridad?	3	3	3	APLICABLE
Análisis	¿Cree usted que la empresa realice análisis forense para la toma de medidas correctivas?	4	4	4	APLICABLE

Variable Dependiente: Concientización digital

Dimensiones del instrumento:

- Primera dimensión: Conocimiento tecnológico
- Objetivos de la Dimensión: Identificar el nivel de conocimiento y el uso que tienen los usuarios respecto a la tecnología.

Indicadores	Ítem	Claridad	Coherencia	Relevancia	Observaciones / Recomendaciones
Comprensión	¿Considera usted que cuenta con un conocimiento básicos de la tecnología y cómo funcionan los dispositivos y aplicaciones digitales?	4	4	4	APLICABLE

Indicadores	Ítem	Claridad	Coherencia	Relevancia	Observaciones / Recomendaciones
Comprensión	¿Considera usted que entiende sobre los riesgos que conlleva las tecnologías digitales, como la privacidad, phishing y malware?	4	4	4	APLICABLE
Usabilidad	¿Considera usted que las herramientas y servicios digitales son intuitivos y están diseñados teniendo en cuenta las necesidades del usuario?	3	3	3	APLICABLE
Usabilidad	¿Considera usted que el acceso a la información y los servicios en línea son convenientes y permiten agilizar actividades?	4	4	4	APLICABLE

- Segunda dimensión: Habilidad digital
- Objetivos de la Dimensión: Identificar la competencia y grado del usuario en los entornos digitales.

Indicadores	Ítem	Claridad	Coherencia	Relevancia	Observaciones / Recomendaciones
Competencia	¿Considera usted que cuenta con habilidades suficientes para utilizar una variedad de aplicaciones y herramientas digitales para realizar tareas y actividades en línea?	3	3	3	APLICABLE
Competencia	¿Considera usted que cuenta con la capacidad de evaluar críticamente la calidad y la veracidad de la información encontrada en Internet?	4	4	4	APLICABLE
Evaluación	¿Considera usted que cuenta con la capacidad de proteger su privacidad y seguridad en línea mediante el uso de configuraciones de privacidad y medidas de seguridad digital?	3	3	3	APLICABLE
Evaluación	¿Considera usted que puede utilizar de manera efectiva las herramientas y recursos para su protección y seguridad digital, como antivirus y contraseñas seguras?	4	4	4	APLICABLE

- Tercera dimensión: Seguridad digital
- Objetivos de la Dimensión: Identificar el nivel de protección y prevención del usuario frente a las actividades en línea.

Indicadores	Ítem	Claridad	Coherencia	Relevancia	Observaciones / Recomendaciones
Protección	¿Cree usted que cuenta con la capacidad de identificar y evitar las principales amenazas en línea, como el phishing y el malware?	4	4	4	APLICABLE
Protección	¿Cree usted que es consciente sobre los riesgos asociados con la divulgación de información personal en línea?	3	3	3	APLICABLE
Prevención	¿Cree usted que puede reconocer y evitar comportamientos de riesgo en línea, como descargar archivos adjuntos sospechosos o hacer clic en enlaces no confiables?	4	4	4	APLICABLE
Prevención	¿Cree usted que es importante mantener sus dispositivos y aplicaciones actualizados con las últimas actualizaciones de seguridad?	4	4	4	APLICABLE

Dr. Alindor Fernando Espinoza Espinoza
DNI N° 06809706

Pd.: el presente formato debe tomar en cuenta:
Williams y Webb (1994) así como Powell (2003), mencionan que no existe un consenso respecto al número de expertos a emplear. Por otra parte, el número de jueces que se debe emplear en un juicio depende del nivel de experticia y de la diversidad del conocimiento. Así, mientras Gable y Wolf (1993), Grant y Davis (1997), y Lynn (1986) (citados en McGartland et al. 2003) sugieren un rango de **2** hasta **20 expertos**, Hyrkäs et al. (2003) manifiestan que **10 expertos** brindarán una estimación confiable de la validez de contenido de un instrumento (cantidad mínimamente recomendable para construcciones de nuevos instrumentos). Si un 80 % de los expertos han estado de acuerdo con la validez de un ítem éste puede ser incorporado al instrumento (Voutilainen & Liukkonen, 1995, citados en Hyrkäs et al. (2003).
Ver : https://www.revistaespacios.com/cited2017/cited2017-23.pdf entre otra bibliografía.

Tercera evaluación

Respetado juez: Usted ha sido seleccionado para evaluar el instrumento "Cuestionario para usuarios administrativos de una empresa Outsourcing". La evaluación del instrumento es de gran relevancia para lograr que sea válido y que los resultados obtenidos a partir de éste sean utilizados eficientemente; aportando al quehacer psicológico. Agradecemos su valiosa colaboración.

1. Datos generales del juez

Nombre del juez:	Juan Francisco Pacheco Torres
Grado profesional:	Maestría ( ) Doctor (x)
Área de formación académica:	Clínica ( ) Social ( ) Educativa ( ) Organizacional (x)
Áreas de experiencia profesional:	INGENIERÍA DE SISTEMAS
Institución donde labora:	Universidad César Vallejo
Tiempo de experiencia profesional en el área:	2 a 4 años ( ) Más de 5 años (x)
Experiencia en Investigación Psicométrica: (si corresponde)	

2. Propósito de la evaluación:

Validar el contenido del instrumento, por juicio de expertos.

3. Datos de la escala (Colocar nombre de la escala, cuestionario o inventario)

Nombre de la Prueba:	Cuestionario para usuarios administrativos de una empresa Outsourcing
Autor:	Angeles Gonzales, Edwin Ivan
Procedencia:	Universidad César Vallejo
Administración:	Formularios de Google
Tiempo de aplicación:	15 minutos
Ámbito de aplicación:	24 ítems: V.D. (12 ítems) y V.I. (12 ítems)
Significación:	Explicar Cómo está compuesta la escala (dimensiones, áreas, ítems por área, explicación breve de cuál es el objetivo de medición)

4. Soporte teórico

Escala / ÁREA	Subescala (dimensiones)	Definición
Gestión de la ciberseguridad	Evaluación de riesgos	Señala que es un proceso de identificación, análisis y valoración donde permite establecer un grado de amenaza y riesgo asociado teniendo en consideración el resultado del proceso y la identificación de los controles adecuados. (Pinzón, 2014).
	Políticas de seguridad	Señala que se trata de declaraciones que cubre la seguridad de los sistemas, los cuales contienen definiciones y delimitaciones de responsabilidades técnicas y empresariales. (Gómez, 2011)
	Supervisión de actividades	Define como una función gerencial que se implementa a nivel operativo de la empresa. El supervisor es un director que dirige las actividades de un gerente no ejecutivo, es decir, una persona que no desempeña funciones administrativas en la empresa. (Chiavenato, 2001)
Concientización digital	Conocimiento tecnológico	Menciona que el conocimiento tecnológico hace referencia a todo tipo de conocimiento tecnológico que no solo abarque temas de informática, sino que va más del campo. (Koehler y Mishra, 2008)
	Habilidad digital	Indica que se trata de un conglomerado de conocimientos, portes, artes, condiciones y destrezas que se necesitan para usar las tecnologías. (Morduchowicz, 2021)
	Seguridad digital	Menciona a la seguridad digital como un compuesto de acciones que sirven para proteger y controlar las comunicaciones, información y datos siempre con la premisa de la triada sobre seguridad de la información. (Hernández, 2022)

5. Presentación de instrucciones para el juez:

A continuación, a usted le presento el cuestionario para usuarios administrativos de una empresa Outsourcing elaborado por Angeles Gonzales Edwin Ivan en el año 2023. De acuerdo con los siguientes indicadores califique cada uno de los ítems según corresponda.

Categoría	Calificación	Indicador
CLARIDAD El ítem se comprende fácilmente, es decir, su sintáctica y semántica son adecuadas.	1. No cumple con el criterio	El ítem no es claro.
	2. Bajo Nivel	El ítem requiere bastantes modificaciones o una modificación muy grande en el uso de las palabras de acuerdo con su significado o por la ordenación de estas.
	3. Moderado nivel	Se requiere una modificación muy específica de algunos de los términos del ítem.
	4. Alto nivel	El ítem es claro, tiene semántica y sintaxis adecuada.
COHERENCIA El ítem tiene relación lógica con la dimensión o indicador que está midiendo.	1. totalmente en desacuerdo (no cumple con el criterio)	El ítem no tiene relación lógica con la dimensión.
	2. Desacuerdo (bajo nivel de acuerdo)	El ítem tiene una relación tangencial /lejana con la dimensión.
	3. Acuerdo (moderado nivel)	El ítem tiene una relación moderada con la dimensión que se está midiendo.
	4. Totalmente de Acuerdo (alto nivel)	El ítem se encuentra está relacionado con la dimensión que está midiendo.
RELEVANCIA El ítem es esencial o importante, es decir debe ser incluido.	1. No cumple con el criterio	El ítem puede ser eliminado sin que se vea afectada la medición de la dimensión.
	2. Bajo Nivel	El ítem tiene alguna relevancia, pero otro ítem puede estar incluyendo lo que mide éste.
	3. Moderado nivel	El ítem es relativamente importante.
	4. Alto nivel	El ítem es muy relevante y debe ser incluido.

Leer con detenimiento los ítems y calificar en una escala de 1 a 4 su valoración, así como solicitamos brindesus observaciones que considere pertinente

1 No cumple con el criterio
2. Bajo Nivel
3. Moderado nivel
4. Alto nivel

Variable Independiente: Gestión de la ciberseguridad

Dimensiones del instrumento:

- Primera dimensión: Evaluación de riesgos
- Objetivos de la Dimensión: Identificar el cumplimiento de la evaluación de riesgos en la empresa Outsourcing.

Indicadores	Ítem	Claridad	Coherencia	Relevancia	Observaciones / Recomendaciones
Exposición	¿Cree usted que la empresa realiza evaluaciones regulares de vulnerabilidades en sus sistemas y redes?	4	4	4	
Exposición	¿Cree usted que la empresa implementa medidas proactivas para mitigar las vulnerabilidades?	4	4	4	
Detección	¿Cree usted que la empresa tiene sistemas de detección de intrusiones en tiempo real?	4	4	4	
Detección	¿Cree usted que la empresa cuenta con un plan de respuesta a incidentes?	4	4	4	

- Segunda dimensión: Políticas de seguridad
- Objetivos de la Dimensión: Identificar la aplicación de las políticas de seguridad en la empresa Outsourcing.

Indicadores	Ítem	Claridad	Coherencia	Relevancia	Observaciones / Recomendaciones
Control	¿Considera usted que las políticas de seguridad establecen claramente los controles y medidas necesarios para proteger la información?	4	4	4	
Control	¿Considera usted que la empresa cuenta con mecanismos de supervisión y control para las políticas de seguridad?	4	4	4	
Documentación	¿Considera usted que las políticas de seguridad son revisadas y validadas para garantizar un correcto estándar de seguridad?	4	4	4	

Indicadores	Ítem	Claridad	Coherencia	Relevancia	Observaciones / Recomendaciones
Documentación	¿Considera usted que la documentación de la gestión de ciberseguridad está actualizada y accesible al personal?	4	4	4	

- Tercera dimensión: Supervisión de actividades
- Objetivos de la Dimensión: Identificar la aplicación de actividades de monitoreo en la empresa Outsourcing.

Indicadores	Ítem	Claridad	Coherencia	Relevancia	Observaciones / Recomendaciones
Monitoreo	¿Cree usted que la empresa cuenta con sistemas y herramientas de monitoreo en tiempo real que detectan y alertan sobre actividades sospechosas en la red y sistemas?	4	4	4	
Monitoreo	¿Cree usted que existen protocolos y procedimientos de respuesta identificados para el monitoreo de actividades?	4	4	4	
Análisis	¿Cree usted que la empresa realiza análisis periódicos de los registros para identificar patrones y tendencias para mejorar la seguridad?	4	4	4	
Análisis	¿Cree usted que la empresa realice análisis forense para la toma de medidas correctivas?	4	4	4	

Variable Dependiente: Concientización digital

Dimensiones del instrumento:

- Primera dimensión: Conocimiento tecnológico
- Objetivos de la Dimensión: Identificar el nivel de conocimiento y el uso que tienen los usuarios respecto a la tecnología.

Indicadores	Ítem	Claridad	Coherencia	Relevancia	Observaciones / Recomendaciones
Comprensión	¿Considera usted que cuenta con un conocimiento básicos de la tecnología y cómo funcionan los dispositivos y aplicaciones digitales?	4	4	4	

Indicadores	Ítem	Claridad	Coherencia	Relevancia	Observaciones / Recomendaciones
Comprensión	¿Considera usted que entiende sobre los riesgos que conlleva las tecnologías digitales, como la privacidad, phishing y malware?	4	4	4	
Usabilidad	¿Considera usted que las herramientas y servicios digitales son intuitivos y están diseñados teniendo en cuenta las necesidades del usuario?	4	4	4	
Usabilidad	¿Considera usted que el acceso a la información y los servicios en línea son convenientes y permiten agilizar actividades?	4	4	4	

- Segunda dimensión: Habilidad digital
- Objetivos de la Dimensión: Identificar la competencia y grado del usuario en los entornos digitales.

Indicadores	Ítem	Claridad	Coherencia	Relevancia	Observaciones / Recomendaciones
Competencia	¿Considera usted que cuenta con habilidades suficientes para utilizar una variedad de aplicaciones y herramientas digitales para realizar tareas y actividades en línea?	4	4	4	
Competencia	¿Considera usted que cuenta con la capacidad de evaluar críticamente la calidad y la veracidad de la información encontrada en Internet?	4	4	4	
Evaluación	¿Considera usted que cuenta con la capacidad de proteger su privacidad y seguridad en línea mediante el uso de configuraciones de privacidad y medidas de seguridad digital?	4	4	4	
Evaluación	¿Considera usted que puede utilizar de manera efectiva las herramientas y recursos para su protección y seguridad digital, como antivirus y contraseñas seguras?	4	4	4	

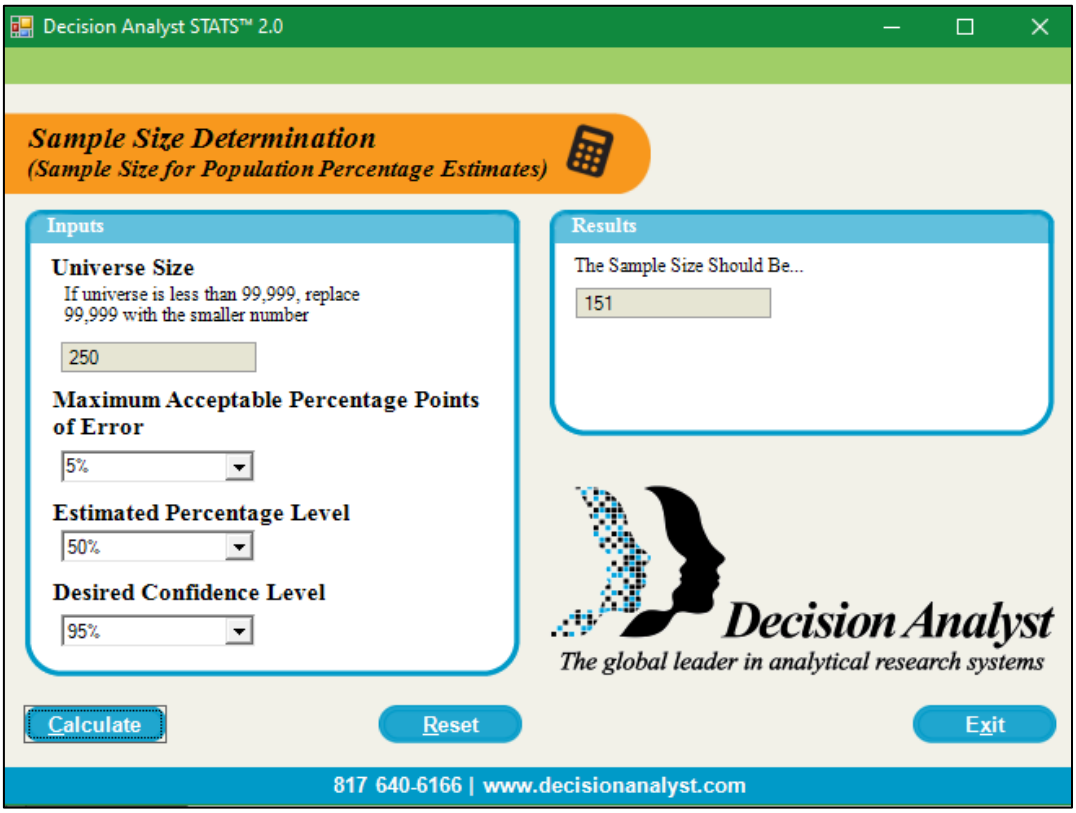
- Tercera dimensión: Seguridad digital
- Objetivos de la Dimensión: Identificar el nivel de protección y prevención del usuario frente a las actividades en línea.

Indicadores	Ítem	Claridad	Coherencia	Relevancia	Observaciones / Recomendaciones
Protección	¿Cree usted que cuenta con la capacidad de identificar y evitar las principales amenazas en línea, como el phishing y el malware?	4	4	4	
Protección	¿Cree usted que es consciente sobre los riesgos asociados con la divulgación de información personal en línea?	4	4	4	
Prevención	¿Cree usted que puede reconocer y evitar comportamientos de riesgo en línea, como descargar archivos adjuntos sospechosos o hacer clic en enlaces no confiables?	4	4	4	
Prevención	¿Cree usted que es importante mantener sus dispositivos y aplicaciones actualizados con las últimas actualizaciones de seguridad?	4	4	4	

Firma del evaluador
DNI: 18167212

Pd.: el presente formato debe tomar en cuenta:
Williams y Webb (1994) así como Powell (2003), mencionan que no existe un consenso respecto al número de expertos a emplear. Por otra parte, el número de jueces que se debe emplear en un juicio depende del nivel de experticia y de la diversidad del conocimiento. Así, mientras Gable y Wolf (1993), Grant y Davis (1997), y Lynn (1986) (citados en McGartland et al. 2003) sugieren un rango de **2** hasta **20 expertos**, Hyrkäs et al. (2003) manifiestan que **10 expertos** brindarán una estimación confiable de la validez de contenido de un instrumento (cantidad mínimamente recomendable para construcciones de nuevos instrumentos). Si un 80 % de los expertos han estado de acuerdo con la validez de un ítem éste puede ser incorporado al instrumento (Voutilainen & Liukkonen, 1995, citados en Hyrkäs et al. (2003).
Ver : https://www.revistaespacios.com/cited2017/cited2017-23.pdf entre otra bibliografía.

Anexo 5: Cálculo de la muestra



Anexo 6: Prueba de confiabilidad

Prueba	N° de encuestas	N° de elementos	Alfa de Cronbach
Piloto	50	24	0.973

Prueba	N° de encuestas	N° de elementos	Alfa de Cronbach
General	151	24	0.978

Anexo 7: Registro de Base de datos

Encuesta	V1-Gestión de la ciberseguridad										V2-Concientización digital													
	D-1			D-2			D-3				D-1				D-2				D-3					
	I-1		I-2		I-3	I-4		I-5	I-6		I-1		I-2		I-3		I-4		I-5		I-6			
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
1	4	3	3	4	4	4	4	3	3	3	3	3	4	3	4	5	4	4	3	4	3	4	4	5
2	3	3	3	2	3	2	3	3	3	3	3	3	3	2	4	4	3	3	3	3	2	2	3	4
3	4	5	4	4	4	4	5	4	4	4	4	4	5	4	4	5	5	4	4	4	4	5	5	5
4	4	4	4	4	4	4	4	2	4	4	3	4	4	3	4	5	4	4	4	3	3	4	4	5
5	4	3	4	3	4	4	3	2	3	3	4	3	4	3	4	5	4	4	4	4	2	3	3	4
6	4	3	4	4	4	4	4	3	3	4	4	4	3	2	4	4	3	2	4	3	2	3	3	4
7	4	4	4	4	4	4	4	4	4	4	4	4	4	3	4	4	4	4	4	3	3	4	4	4
8	4	4	3	3	4	3	4	3	3	3	3	3	4	3	3	4	3	3	3	3	2	3	3	4
9	4	4	4	4	4	4	3	3	4	4	3	3	4	3	4	4	4	4	4	4	3	4	4	5
10	4	4	5	4	4	4	4	4	4	4	4	4	4	4	4	5	4	4	4	4	4	5	4	5
11	4	3	4	3	3	4	4	2	3	3	4	3	4	2	4	4	3	3	3	2	2	3	3	4
12	5	4	5	5	5	4	5	4	5	5	4	5	5	4	5	5	5	5	5	5	4	5	5	5
13	4	4	5	4	5	5	4	5	4	5	5	4	5	4	5	5	4	4	5	4	4	4	5	5
14	4	4	4	4	4	4	4	3	4	3	3	3	4	3	3	4	3	3	4	3	2	3	3	4
15	4	3	4	3	3	3	3	2	3	3	3	3	4	2	4	4	3	3	3	3	2	3	3	3
16	3	3	3	3	3	3	3	2	3	3	3	3	3	1	3	4	3	3	3	3	1	3	3	3
17	3	2	3	3	3	2	3	1	3	3	3	3	4	2	4	4	3	3	3	3	2	3	3	4
18	4	3	3	4	3	4	3	3	4	3	3	3	4	3	4	5	4	3	3	3	3	4	4	5
19	3	3	3	3	2	3	3	3	3	2	3	2	4	2	4	3	3	4	4	3	2	4	3	4
20	3	2	3	3	3	3	3	1	3	3	3	2	3	1	3	3	3	3	3	2	3	3	2	3
21	3	3	2	3	3	3	3	4	3	3	3	2	3	2	3	3	3	4	3	3	2	3	3	3
22	4	3	4	4	4	3	3	2	4	3	4	3	4	3	4	4	4	4	4	4	2	4	3	4
23	3	2	3	3	3	3	3	1	3	3	3	3	3	1	3	4	3	3	3	2	1	3	3	3
24	4	3	4	4	4	4	4	3	4	4	4	3	4	3	4	4	4	4	4	3	3	4	4	5
25	3	2	3	3	3	2	3	2	3	3	2	2	4	3	3	5	4	3	4	3	3	3	4	5
26	3	3	3	3	2	3	3	1	3	3	3	3	4	2	3	4	3	3	3	3	1	3	2	3
27	3	3	2	2	2	3	2	1	3	3	3	2	3	1	3	4	3	3	3	2	1	3	2	3
28	4	3	4	4	3	4	4	3	4	4	4	4	4	4	4	5	4	4	4	3	3	4	4	5
29	4	4	4	4	4	4	4	4	4	5	4	4	4	4	4	4	4	4	4	3	4	4	4	4
30	3	3	3	2	3	3	3	2	3	3	3	3	3	1	3	4	3	3	2	3	1	3	3	3
31	4	3	3	4	3	3	4	3	3	3	3	3	4	3	3	4	3	3	3	3	3	3	3	4
32	3	3	3	3	2	3	3	2	3	3	3	3	3	2	3	4	3	3	3	2	2	3	3	3
33	4	4	4	4	5	4	4	4	4	4	4	4	4	3	4	4	4	4	4	4	3	4	4	5
34	4	3	3	4	3	3	4	4	4	4	3	3	4	2	4	3	3	3	3	4	2	4	3	4
35	3	3	4	3	3	4	3	4	3	3	3	2	3	1	3	3	3	2	3	3	2	3	2	2
36	4	3	3	3	3	3	4	3	4	3	3	3	4	3	3	4	4	3	3	3	3	3	3	4
37	4	4	4	4	4	4	4	5	4	4	4	4	4	3	4	4	4	4	4	4	4	4	4	5
38	3	2	3	3	2	3	3	3	3	2	2	3	3	2	3	3	2	2	3	3	2	3	3	3
39	3	3	3	2	3	3	3	3	3	3	2	3	3	1	3	2	3	3	3	2	2	3	3	3
40	4	3	3	4	3	3	4	3	3	3	3	3	4	3	4	4	3	3	4	3	3	4	4	4
41	3	3	2	2	3	3	3	1	3	3	2	2	3	1	2	3	2	2	2	2	1	2	2	2
42	4	3	3	4	3	4	4	4	3	4	3	3	3	3	3	4	3	3	4	4	3	4	3	4
43	3	4	3	3	4	3	4	4	3	4	3	3	4	3	4	4	4	3	4	3	4	4	4	5
44	4	4	4	4	4	4	4	3	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	5

Encuesta	V1-Gestión de la ciberseguridad										V2-Concientización digital													
	D-1			D-2			D-3				D-1				D-2				D-3					
	I-1		I-2		I-3		I-4		I-5	I-6		I-1		I-2		I-3		I-4		I-5		I-6		
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
45	3	3	3	3	3	3	3	3	3	3	3	2	3	2	2	2	3	3	2	3	2	3	2	3
46	3	3	3	2	3	3	2	1	3	3	2	3	3	1	3	2	3	2	2	2	3	2	3	2
47	4	4	3	5	4	5	4	4	4	4	4	4	4	4	4	4	4	4	5	4	4	4	4	5
48	4	4	3	4	4	4	3	3	4	4	3	3	3	2	3	4	3	3	3	3	2	3	4	4
49	3	2	2	2	3	3	2	2	2	2	2	2	3	1	3	3	2	3	3	2	1	2	2	2
50	4	3	4	3	3	4	3	3	3	3	3	3	4	4	4	4	4	3	4	4	3	4	4	5
51	3	3	3	3	2	3	3	1	3	3	3	3	3	2	2	2	3	2	2	2	3	2	3	3
52	4	4	3	4	3	3	3	3	4	4	3	3	4	3	4	4	4	4	4	3	3	4	4	4
53	3	3	4	3	3	3	3	2	3	3	3	3	3	1	3	2	3	2	2	1	3	2	3	3
54	4	4	4	4	4	4	4	4	4	4	4	4	4	3	4	4	3	4	3	3	4	4	4	5
55	5	5	5	4	5	5	5	5	5	5	4	4	5	4	5	5	5	5	5	5	5	4	5	5
56	4	3	4	4	3	3	4	2	4	3	3	3	4	3	3	4	3	3	3	3	3	4	3	4
57	3	2	2	2	2	2	2	3	2	2	2	2	3	1	3	3	3	3	3	3	1	3	3	2
58	3	4	4	4	4	3	4	4	4	3	4	4	4	3	4	4	4	4	4	3	3	4	4	4
59	3	3	3	3	3	3	3	2	3	3	3	3	3	2	3	3	3	3	3	2	2	3	3	3
60	4	4	4	3	4	4	4	3	4	4	4	4	4	3	4	4	4	4	4	4	3	4	4	4
61	3	3	3	2	3	2	3	1	2	2	3	2	3	1	3	3	2	3	3	3	1	3	3	3
62	4	4	4	4	5	4	4	3	4	4	4	4	4	3	3	5	3	4	4	3	3	4	4	5
63	4	4	4	4	5	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4
64	4	4	3	4	4	3	3	3	4	3	4	4	3	3	3	3	3	3	4	3	3	3	3	3
65	3	3	2	3	3	3	2	2	3	3	3	2	3	3	2	3	3	3	3	2	3	3	3	2
66	3	3	3	2	3	3	2	3	2	3	3	3	3	1	3	3	1	1	3	2	1	2	2	2
67	2	2	2	2	2	2	2	2	2	2	2	2	3	1	3	3	2	2	3	2	1	2	2	2
68	5	5	5	5	5	5	5	5	5	5	5	5	4	4	4	4	4	3	4	4	3	4	4	5
69	3	3	3	2	3	2	3	1	3	3	2	2	3	3	3	3	3	3	3	3	2	3	3	3
70	3	3	4	3	3	3	3	3	2	3	3	2	3	2	3	2	3	3	3	2	2	3	2	2
71	3	2	2	2	2	2	2	2	2	2	2	2	2	1	2	1	2	2	2	2	1	2	2	2
72	4	3	3	3	4	4	4	4	3	4	3	3	4	3	4	4	4	4	4	4	3	4	4	4
73	3	3	3	3	2	3	3	2	3	3	3	3	3	2	3	3	3	3	3	3	3	3	3	3
74	3	2	2	3	2	2	2	1	2	2	2	2	3	2	3	2	2	2	2	3	2	3	3	2
75	4	4	4	4	4	4	4	4	4	4	4	4	4	3	4	4	4	4	4	3	3	4	4	4
76	4	3	4	4	4	4	4	3	4	4	4	3	4	3	3	3	4	3	4	3	3	4	4	4
77	3	3	3	3	2	3	3	2	3	3	3	2	3	2	3	3	3	3	3	3	2	3	3	3
78	3	3	3	3	3	4	3	3	3	3	3	2	4	3	4	3	3	3	3	2	3	3	3	4
79	4	4	3	4	4	4	3	4	4	4	4	3	3	3	3	3	4	3	3	3	2	3	3	4
80	4	4	3	3	4	4	3	4	4	3	4	3	4	3	4	4	4	4	4	4	3	4	4	4
81	4	3	3	3	4	4	4	2	4	3	3	3	4	3	3	3	3	3	3	3	3	3	3	3
82	3	3	3	3	3	2	3	2	3	3	3	3	3	2	3	3	3	2	2	3	2	3	3	3
83	4	4	3	4	4	4	3	4	4	4	4	3	4	3	3	3	4	3	3	4	3	4	4	5

Encuesta	V1-Gestión de la ciberseguridad										V2-Concientización digital													
	D-1			D-2			D-3				D-1				D-2				D-3					
	I-1		I-2		I-3	I-4		I-5		I-6	I-1		I-2		I-3		I-4		I-5		I-6			
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
84	4	4	4	3	4	5	4	4	4	4	4	4	4	3	4	4	4	3	4	3	3	4	4	4
85	3	3	2	3	3	2	2	3	3	3	3	3	3	2	3	3	3	3	3	3	2	3	3	3
86	3	2	2	2	2	2	2	2	2	2	2	2	2	1	2	2	2	1	1	2	1	2	2	2
87	4	4	4	4	5	4	4	4	4	3	4	4	4	3	4	4	4	4	4	4	3	4	4	4
88	4	3	3	4	5	4	4	3	4	4	4	4	3	2	3	4	3	3	4	4	2	3	3	4
89	4	4	5	5	4	5	4	4	5	4	4	4	5	4	5	5	5	4	5	5	4	5	5	5
90	3	3	3	3	4	3	3	3	3	3	3	3	3	2	3	3	3	3	3	3	2	3	3	3
91	3	3	3	2	4	3	3	2	3	3	3	3	3	3	3	3	3	2	3	3	2	3	3	3
92	4	4	4	4	5	4	4	4	4	4	4	4	3	3	3	2	3	3	2	3	2	3	3	4
93	3	3	2	3	3	2	3	3	3	3	3	3	3	2	3	3	3	3	3	3	3	3	3	3
94	4	3	3	4	4	4	3	4	4	4	3	3	3	3	3	3	3	3	3	3	2	3	3	4
95	3	3	3	3	4	3	3	1	3	3	3	3	3	1	3	3	2	3	2	3	1	3	3	2
96	3	3	4	3	3	3	3	2	3	3	3	2	3	2	3	3	3	3	3	3	2	3	3	3
97	3	3	3	2	3	2	3	2	3	3	3	3	3	2	3	3	3	3	3	3	2	2	3	3
98	4	3	4	4	4	4	3	2	4	3	4	3	3	1	3	2	3	3	3	2	2	3	2	2
99	3	2	3	3	4	3	2	2	3	3	3	3	3	2	2	2	3	3	2	2	2	3	3	3
100	3	3	2	2	3	3	2	1	2	2	2	2	3	1	2	2	3	2	2	2	2	3	2	2
101	4	4	3	4	5	4	4	3	4	4	4	4	4	3	4	4	4	4	4	4	3	3	4	5
102	3	4	3	3	4	4	3	3	3	3	4	3	4	4	3	3	3	4	4	4	3	4	3	4
103	3	3	3	2	3	3	3	3	3	3	3	3	3	3	3	3	4	3	3	3	2	3	3	4
104	4	4	3	4	4	4	4	4	3	4	4	4	4	3	4	4	4	4	4	3	3	4	4	4
105	3	3	3	2	3	3	3	3	2	3	2	3	3	2	3	3	2	2	3	2	2	3	3	3
106	4	4	5	4	5	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	3	4	4	4
107	4	3	3	3	3	4	3	3	3	3	3	3	4	3	3	4	3	3	3	3	3	3	3	4
108	4	4	4	4	4	4	4	4	4	4	4	4	4	3	4	4	4	4	4	4	4	4	4	4
109	3	2	3	3	4	2	3	3	3	3	3	2	3	2	3	3	3	3	3	3	2	3	3	3
110	3	3	4	3	4	3	4	2	3	4	3	3	3	3	3	3	3	3	3	3	2	3	3	3
111	3	3	3	3	2	3	3	1	3	3	3	2	3	2	3	3	2	3	3	2	1	2	2	3
112	3	3	3	3	3	3	3	3	3	3	3	3	3	2	3	3	3	3	3	3	3	3	3	3
113	3	3	3	2	2	3	2	3	3	3	3	3	3	2	2	3	3	3	3	3	2	3	3	3
114	5	5	5	5	5	5	5	5	4	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5
115	4	4	3	4	3	4	4	4	4	4	4	3	3	3	3	3	2	3	3	3	2	3	3	3
116	3	3	2	2	3	3	2	2	3	2	2	2	3	2	2	2	2	2	2	2	1	2	2	2
117	3	3	3	2	3	3	3	3	3	3	3	2	3	3	3	3	3	3	3	3	3	3	2	3
118	3	3	3	2	3	2	3	1	3	3	3	3	3	2	3	3	3	3	3	2	2	3	3	3
119	3	3	3	3	3	3	3	2	3	3	3	3	3	2	3	3	3	3	3	3	2	3	3	3
120	4	4	5	4	4	4	4	4	4	4	4	4	4	3	4	4	4	4	4	4	4	4	4	4
121	3	3	2	3	3	3	3	2	3	3	3	2	3	1	3	2	3	3	3	3	2	3	3	3

Encuesta	V1-Gestión de la ciberseguridad										V2-Concientización digital													
	D-1			D-2			D-3				D-1				D-2				D-3					
	I-1		I-2		I-3		I-4		I-5	I-6		I-1		I-2		I-3		I-4		I-5		I-6		
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
122	3	3	3	3	4	3	3	3	3	3	3	2	3	3	3	3	3	3	3	3	2	3	3	4
123	3	3	3	3	3	3	3	1	3	3	3	3	3	2	3	2	2	3	2	2	2	3	3	2
124	4	3	4	4	4	4	4	3	4	4	4	3	4	3	4	4	4	3	3	4	3	4	3	5
125	3	3	2	3	3	3	3	2	3	3	3	2	3	2	2	3	3	3	2	2	2	3	3	3
126	3	3	3	3	4	3	3	3	3	3	3	3	3	2	3	3	3	3	3	3	2	2	3	3
127	4	3	4	4	5	4	3	4	4	4	3	3	4	4	4	4	3	4	4	4	3	4	4	4
128	5	5	4	5	5	5	5	5	4	5	5	5	5	4	5	4	4	5	5	5	4	5	5	5
129	4	4	4	4	4	4	4	4	4	4	3	4	4	3	4	4	4	4	4	4	4	4	4	5
130	3	2	3	3	3	3	3	3	2	3	2	2	3	2	2	3	3	2	3	3	2	3	2	3
131	3	2	3	3	4	3	3	2	3	3	3	3	3	3	3	3	3	3	3	3	2	3	3	4
132	3	3	2	3	4	3	2	1	3	2	3	3	3	2	3	3	3	3	2	3	2	3	2	3
133	4	3	3	4	3	3	3	2	3	3	3	3	3	2	3	3	3	3	3	3	2	3	3	3
134	3	3	3	2	3	3	2	1	2	3	3	2	3	1	3	3	3	3	3	3	2	3	4	4
135	4	3	4	4	5	4	4	3	4	4	4	4	4	3	4	4	4	4	4	4	3	4	4	5
136	4	4	4	3	4	4	4	4	4	4	4	4	4	4	4	5	4	4	4	4	3	4	4	4
137	4	4	4	4	5	4	4	3	4	4	4	4	4	3	3	4	3	3	4	4	3	4	4	4
138	3	3	3	3	4	3	3	3	3	3	3	2	3	2	3	3	3	3	3	3	2	3	3	3
139	3	2	3	3	4	3	4	3	3	3	4	4	3	3	3	4	3	4	3	3	3	3	3	4
140	4	4	3	4	4	4	3	4	4	4	4	3	3	2	3	3	3	3	3	3	2	3	3	4
141	3	2	2	2	3	2	2	1	2	2	2	2	2	1	2	2	2	2	2	2	1	3	2	2
142	3	3	3	2	3	3	3	3	3	3	3	3	3	2	2	3	3	3	3	3	2	3	3	3
143	3	2	3	2	2	3	3	3	3	3	3	3	3	1	3	2	3	3	3	3	1	3	2	3
144	3	3	3	3	4	3	3	2	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3
145	3	4	3	3	1	2	3	3	2	2	3	3	3	1	3	3	3	3	3	2	1	3	3	3
146	4	3	4	3	4	4	4	3	3	3	4	3	4	3	4	4	4	3	3	4	3	4	3	4
147	3	3	2	3	2	3	2	2	2	3	2	2	3	1	2	2	2	3	2	2	1	2	2	2
148	3	3	3	2	3	3	3	2	3	3	3	2	3	2	2	3	3	3	2	2	1	3	3	2
149	3	2	2	2	1	3	3	3	2	3	3	2	3	2	3	3	3	3	3	3	2	3	3	3
150	3	3	3	3	3	3	3	2	3	3	3	3	3	2	3	3	3	3	3	3	3	3	3	3
151	4	4	3	4	4	4	4	4	4	4	4	3	4	3	4	4	4	4	4	3	4	4	4	4

Anexo 8: Formato de referencias bibliográficas

Requisitos	Total
Cantidad de referencias	53
Últimos 7 años	70%
Revistas científicas (Artículos)	70%
Libros o Tesis	30%
Ingles u otro idioma	40%