UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA
FACULTAD DE SISTEMAS Y TELECOMUNICACIONES INSTITUTO DE POSTGRADO

TÍTULO

Análisis del Impacto de la Formación en Ciberseguridad sobre Prácticas y Detección en Salud Pública

AUTOR

Arévalo Llaguno, Angel Ariel

TRABAJO DE TITULACIÓN

Previo a la obtención del grado académico en
MAGÍSTER EN CIBERSEGURIDAD

TUTOR

Suárez Riofrío, Patricia Leonor

Santa Elena, Ecuador
Año 2026

UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA
FACULTAD DE SISTEMAS Y TELECOMUNICACIONES
INSTITUTO DE POSTGRADO

TRIBUNAL DE SUSTENTACIÓN

Validar únicamente en FirmaEC.
Firmado electrónicamente por:
ALICIA GERMANIA ANDRADE VERA

Ing. Alicia Andrade Vera, Mgtr.
COORDINADORA DEL PROGRAMA

Validar únicamente en FirmaEC.
Firmado electrónicamente por:
PATRICIA LEONOR SUAREZ RIOFRIO

Ing. Patricia Suarez Riofrío, Ph.D.
TUTOR

Validar únicamente en FirmaEC.
Firmado electrónicamente por:
JAIME BENJAMIN OROZCO IGUASNIA

Ing, Jaime Orozco Iguasnia, Mgtr.
DOCENTE ESPECIALISTA

Validar únicamente en FirmaEC.
Firmado electrónicamente por:
ALFREDO RAMON TUMBACO REYES

Ing. Alfredo Tumbaco Reyes, Mgtr.
DOCENTE ESPECIALISTA

Validar únicamente en FirmaEC.
Firmado electrónicamente por:
MARIA MARGARITA RIVERA GONZALEZ

Abg. María Rivera González, Mgtr.
SECRETARIA GENERAL
UPSE

UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA
FACULTAD DE SISTEMAS Y TELECOMUNICACIONES
INSTITUTO DE POSTGRADO

CERTIFICACIÓN

Certifico que luego de haber dirigido científica y técnicamente el desarrollo y estructura final del trabajo, este cumple y se ajusta a los estándares académicos, razón por el cual apruebo en todas sus partes el presente trabajo de titulación que fue realizado en su totalidad por **AREVALO LLAGUNO ANGEL ARIEL**, como requerimiento para la obtención del título de Magíster en Ciberseguridad.

TUTOR

Validar únicamente en FirmaEC.
Firmado electrónicamente por:
PATRICIA LEONOR SUAREZ RIOFRIO

Ing. Patricia Suarez Riofrío, Ph.D.

Santa Elena, 30 de junio del 2026

UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA
FACULTAD DE SISTEMAS Y TELECOMUNICACIONES
INSTITUTO DE POSTGRADO

DECLARACIÓN DE RESPONSABILIDAD

Yo, **ANGEL ARIEL AREVALO LLAGUNO**

DECLARO QUE:

El trabajo de Titulación, **ANÁLISIS DEL IMPACTO DE LA FORMACIÓN EN CIBERSEGURIDAD SOBRE PRÁCTICAS Y DETECCIÓN EN SALUD PÚBLICA,** previo a la obtención del título en Magíster en Ciberseguridad, ha sido desarrollado respetando derechos intelectuales de terceros conforme las citas que constan en el documento, cuyas fuentes se incorporan en las referencias o bibliografías. Consecuentemente este trabajo es de mi total autoría.

En virtud de esta declaración, me responsabilizo del contenido, veracidad y alcance del Trabajo de Titulación referido.

Santa Elena, 30 de junio del 2026

EL AUTOR

Validar únicamente en FirmaEC.
Firmado electrónicamente por:
ANGEL ARIEL AREVALO LLAGUNO

Arévalo Llaguno Angel Ariel

UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA
FACULTAD DE CIENCIAS DE LA INGENIERÍA
INSTITUTO DE POSTGRADO

CERTIFICACIÓN DE ANTIPLAGIO

Certifico que después de revisar el documento final del trabajo de titulación denominado "**ANÁLISIS DEL IMPACTO DE LA FORMACIÓN EN CIBERSEGURIDAD SOBRE PRÁCTICAS Y DETECCIÓN EN SALUD PÚBLICA**", presentado por el estudiante, **AREVALO LLAGUNO ANGEL ARIEL** fue enviado al Sistema Antiplagio COMPILATIO, presentando un porcentaje de similitud correspondiente al 3%, por lo que se aprueba el trabajo para que continúe con el proceso de titulación.


Analysis attestation
Compilatio Magister+ | UPSE-ECU

Formato_AREVALO_LLAGUNO_FINAL
ID : 1067567b346696b725ed8162ae38602f43bcef37

3%
Suspicious texts

File name : Formato_AREVALO_LLAGUNO_FINAL.txt
Original file size : 1.29 MB
Number of words : 15,176

Submitter : PATRICIA LEONOR SUAREZ RIOFRIO
Submission date : June 29, 2026
Upload type : interface
analysis end date : June 29, 2026

TUTOR

Validar únicamente en FirmaEC.
Firmado electrónicamente por:
PATRICIA LEONOR SUAREZ RIOFRIO

Ing. Patricia Suarez Riofrío, Ph.D.

UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA
FACULTAD DE SISTEMAS Y TELECOMUNICACIONES
INSTITUTO DE POSTGRADO

AUTORIZACIÓN

Yo, **AREVALO LLAGUNO ANGEL ARIEL**

Autorizo a la Universidad Estatal Península de Santa Elena, para que haga de este trabajo de titulación o parte de él, un documento disponible para su lectura consulta y procesos de investigación, según las normas de la Institución.

Cedo los derechos en línea patrimoniales de examen de carácter complexivo con fines de difusión pública, además apruebo la reproducción de este examen de carácter complexivo dentro de las regulaciones de la Universidad, siempre y cuando esta reproducción no suponga una ganancia económica y se realice respetando mis derechos de autor.

Santa Elena, 30 de junio del 2026

EL AUTOR

Validar únicamente en FirmaEC.
Firmado electrónicamente por:
ANGEL ARIEL AREVALO LLAGUNO

Arévalo Llaguno Angel Ariel

AGRADECIMIENTO

Agradezco profundamente a mis padres y familia, quienes han sido mi pilar fundamental a lo largo de este proceso académico. Su apoyo incondicional, comprensión y motivación constante me han permitido superar cada obstáculo y alcanzar esta meta tan importante.

Expreso mi gratitud a mi tutora, Patricia Leonor Suárez Riofrío, por su guía, paciencia y valiosas sugerencias, que han enriquecido significativamente el desarrollo de este trabajo. Su dedicación y compromiso han sido esenciales para mi formación profesional y personal.

Agradezco también a los docentes de la Universidad Estatal Península de Santa Elena, quienes con su conocimiento y vocación han contribuido a mi crecimiento académico. Cada enseñanza recibida ha dejado una huella imborrable en mi trayectoria.

Reconozco el apoyo de mis compañeros y amigos, quienes compartieron conmigo momentos de esfuerzo, aprendizaje y compañerismo. Su amistad y colaboración han hecho de este camino una experiencia más llevadera y enriquecedora.

Finalmente, extiendo mi agradecimiento a todas las instituciones y profesionales de la salud que participaron en este estudio, por su disposición y colaboración, sin las cuales este trabajo no habría sido posible.

A todos, mi más sincero agradecimiento.

Angel Ariel Arévalo Llaguno

DEDICATORIA

Dedico este trabajo a mis padres, quienes con su amor, paciencia y ejemplo me han enseñado a nunca rendirme y a perseguir mis sueños con determinación. Gracias por su apoyo incondicional, por creer en mí y por brindarme las herramientas necesarias para crecer tanto personal como profesionalmente.

A mi familia, por ser mi refugio y mi fuente constante de motivación. Su comprensión, cariño y palabras de aliento han sido fundamentales en cada etapa de este proceso académico.

A mis amigos, quienes han estado a mi lado en los momentos más exigentes, ofreciéndome su apoyo, su confianza y su amistad sincera. Gracias por las conversaciones, los consejos y por ayudarme a mantener el equilibrio entre el estudio y la vida personal.

A mis docentes y tutora, especialmente quien guió este trabajo, por su dedicación, orientación y por inspirarme a buscar la excelencia. Su compromiso con la educación y su pasión por el conocimiento han dejado una huella imborrable en mi formación.

Finalmente, dedico este logro a todas las personas que, de una u otra manera, han contribuido a mi desarrollo y me han impulsado a superar cada desafío. Este esfuerzo es también suyo, y espero que mi trabajo sea motivo de orgullo y gratitud para quienes me acompañaron en este camino.

Angel Ariel Arévalo Llaguno

ÍNDICE GENERAL

RESUMEN

La creciente digitalización del sector salud en Ecuador incrementa la exposición a riesgos cibernéticos, en especial en hospitales públicos y rurales donde persisten limitaciones tecnológicas y escasez de personal especializado. En este contexto, la formación en ciberseguridad constituye una estrategia clave para reducir vulnerabilidades, fomentar prácticas seguras y fortalecer el reporte oportuno de incidentes. No obstante, la evidencia empírica sobre su impacto en el sistema sanitario público es limitada. El presente estudio analiza la relación entre la capacitación en ciberseguridad, la adopción de medidas de protección digital y la frecuencia de reporte de vulnerabilidades. Para ello, se aplica un cuestionario estructurado a 50 profesionales de salud distribuidos en tres provincias del Ecuador, bajo un enfoque cuantitativo, con diseño no experimental, correlacional y transversal. El instrumento mide dimensiones de reacción, aprendizaje percibido y aplicabilidad. Los resultados identifican factores que condicionan la efectividad de los programas formativos y sustentan recomendaciones orientadas a fortalecer la ciberseguridad en el sistema sanitario ecuatoriano.

Palabras claves:

ciberseguridad; capacitación en ciberseguridad; sector salud; protección de datos

ABSTRACT

The increasing digitalization of the healthcare sector in Ecuador is increasing exposure to cyber risks, especially in public and rural hospitals where technological limitations and a shortage of specialized personnel persist. In this context, cybersecurity training is a key strategy for reducing vulnerabilities, promoting secure practices, and strengthening the timely reporting of incidents. However, empirical evidence on its impact on the public healthcare system is limited. This study analyzes the relationship between cybersecurity training, the adoption of digital protection measures, and the frequency of vulnerability reporting. To this end, a structured questionnaire was administered to 50 healthcare professionals from three provinces, using a quantitative approach with a non-experimental, correlational, and cross-sectional design. The instrument measures dimensions of reaction, perceived learning, and applicability. The results identify factors that influence the effectiveness of training programs and support recommendations aimed at strengthening cybersecurity in the Ecuadorian healthcare system.

Keywords:

cybersecurity; cybersecurity training; healthcare sector; data protection

INTRODUCCIÓN

La creciente digitalización del sector salud en Ecuador ha transformado la gestión de datos clínicos y administrativos, generando beneficios en eficiencia y acceso a la información, pero también incrementando la exposición a riesgos cibernéticos. Esta realidad es especialmente crítica en hospitales públicos y centros rurales, donde las limitaciones de infraestructura y la escasez de personal especializado aumentan la vulnerabilidad frente a incidentes de seguridad.

En el panorama actual, la ciberseguridad del sector salud enfrenta una presión creciente. El informe Cost of a Data Breach 2025 de IBM identifica a la salud como la industria con el costo promedio más alto por brecha de datos a nivel mundial durante catorce años consecutivos, con cifras cercanas a los 7.4 millones de dólares por incidente y tiempos de detección y contención que superan los nueve meses (IBM, 2025). El mismo informe advierte que la inteligencia artificial ya interviene en una de cada seis brechas reportadas globalmente, principalmente mediante correos de phishing generados de forma automática y suplantación de identidad por deepfake, lo que reduce drásticamente el tiempo y la pericia que un atacante necesita para engañar a un empleado (IBM, 2025). En paralelo, el ransomware continúa afectando a hospitales y clínicas en todo el mundo, con demandas de rescate que en 2025 promediaron más de 5 millones de dólares por incidente (IBM, 2025). Este escenario refuerza la urgencia de fortalecer, mediante la capacitación, la primera línea de defensa frente a estas amenazas: el propio personal de salud.

El objetivo central de este trabajo es analizar el impacto de la capacitación en ciberseguridad sobre la adopción de prácticas seguras y la frecuencia de reportes de vulnerabilidades en instituciones de salud pública. El alcance se circunscribe a tres provincias representativas del sistema sanitario ecuatoriano, mediante un enfoque cuantitativo, correlacional y transversal, que permite establecer asociaciones entre formación recibida y comportamientos del personal.

La tesis plantea que la capacitación en ciberseguridad se asocia significativamente con el fortalecimiento de la cultura de seguridad digital, al contribuir a la reducción de riesgos y al mejor resguardo de datos sensibles. En este marco, se analiza la influencia de la

formación sobre la adopción de medidas de protección específicas —como el uso de contraseñas robustas, la autenticación multifactor y la actualización oportuna de sistemas—, así como sobre la disposición del personal para identificar y reportar incidentes de seguridad.

La investigación adquiere relevancia en los ámbitos social, profesional y científico, al generar evidencia empírica sobre un tema aun insuficientemente abordado en el contexto ecuatoriano. En el plano social, se orienta a la protección de la información de pacientes, especialmente en entornos institucionales vulnerables. En el plano profesional, aporta lineamientos para fortalecer la gestión y las prácticas de seguridad a nivel organizacional. En el plano científico, contribuye a reducir brechas en la literatura sobre ciberseguridad aplicada al sector salud mediante resultados cuantificables y contextualizados.

En cuanto a su aporte, los resultados permiten formular recomendaciones para el diseño de políticas públicas y programas formativos adaptados al contexto nacional, con el propósito de fortalecer la resiliencia digital del sistema sanitario.

Este trabajo se organiza en cuatro capítulos principales que integran el desarrollo completo de la investigación:

1. **En el primer capítulo** se presentan los antecedentes, el planteamiento del problema, los objetivos y la justificación del estudio, estableciendo el marco contextual y la relevancia de la capacitación en ciberseguridad dentro del sector salud público ecuatoriano.
2. **En el segundo capítulo** se expone el marco teórico y referencial, donde se revisan estudios internacionales y regionales, modelos de evaluación del impacto educativo, teorías psicosociales aplicadas al cambio de conducta, así como estándares y buenas prácticas de ciberseguridad aplicables al ámbito sanitario.
3. **En el tercer capítulo** se describe la metodología empleada, detallando el diseño de investigación, la población y muestra seleccionada, los instrumentos de recolección de datos, las variables e indicadores definidos, y el procedimiento de análisis aplicado para evaluar la relación entre capacitación y prácticas seguras.

4. **En el cuarto capítulo** se presentan los resultados obtenidos, acompañados de su análisis y discusión crítica, orientados a identificar los factores que inciden en la efectividad de la capacitación. Finalmente, se incluyen las conclusiones y recomendaciones, que sintetizan los hallazgos y proponen acciones estratégicas para fortalecer la ciberseguridad en el sistema de salud ecuatoriano.

CAPÍTULO I: FUNDAMENTACIÓN

1.1 FUNDAMENTACIÓN

1.1.1 ANTECEDENTES

La transformación digital del sector salud ha generado una creciente dependencia de sistemas informáticos para la gestión de datos clínicos, administrativos y personales. Este proceso ha traído consigo beneficios significativos en términos de eficiencia operativa, acceso oportuno a la información y mejora en la calidad de los servicios. Sin embargo, también ha incrementado la exposición a riesgos cibernéticos que afectan la integridad, disponibilidad y confidencialidad de los datos sensibles de los pacientes.

A nivel internacional, diversos estudios han evidenciado que el sector sanitario es uno de los más vulnerables frente a incidentes de ciberseguridad. Investigaciones como las de (Kruse et al., 2017) y (Karjalainen & Siponen, 2019) muestran que la capacitación en ciberseguridad puede reducir de manera significativa la ocurrencia de incidentes, mejorar la detección de amenazas y fomentar el reporte voluntario de vulnerabilidades. En Europa, el Instituto Nacional de Ciberseguridad (INCIBE, 2024) reporta que el 8% de los ataques registrados afectan al sector salud, siendo el ransomware el más frecuente.

En América Latina, la literatura señala que la falta de infraestructura tecnológica, la sobrecarga laboral y la escasa continuidad en los procesos formativos limitan la efectividad de los programas de capacitación (OEA & BID, 2020; OPS, 2021); En países como Perú, Bolivia y México se han identificado brechas significativas entre el conocimiento teórico adquirido y su aplicación práctica en los entornos hospitalarios.

En el contexto ecuatoriano, aunque se han implementado iniciativas como la Estrategia Nacional de Ciberseguridad (Ministerio de Telecomunicaciones, 2022), aún existe una carencia de estudios empíricos que evalúen el impacto real de la formación en ciberseguridad sobre las prácticas seguras y el reporte de vulnerabilidades en instituciones públicas de salud. Esta ausencia de evidencia limita la formulación de políticas públicas efectivas y la adaptación de programas formativos a las necesidades específicas del sistema sanitario nacional.

Por ello, resulta pertinente desarrollar investigaciones que analicen la relación entre la capacitación en ciberseguridad y la adopción de prácticas seguras en el personal de salud, con el fin de generar datos que permitan fortalecer la resiliencia digital del sector y garantizar la protección de la información en contextos vulnerables.

1.2 DESCRIPCIÓN DEL PROYECTO

El presente proyecto se centra en el análisis del impacto de la capacitación en ciberseguridad sobre las prácticas seguras y el reporte de vulnerabilidades en instituciones de salud pública en Ecuador**.** La investigación surge de la necesidad de evaluar cómo la formación especializada puede influir en la cultura de seguridad digital del personal sanitario, especialmente en hospitales públicos y centros rurales que enfrentan limitaciones de infraestructura tecnológica y escasez de personal especializado.

El estudio se desarrolla bajo un enfoque cuantitativo, diseño no experimental, correlacional y transversal, aplicando un cuestionario estructurado a una muestra estratificada de carácter exploratorio conformada por 50 profesionales de salud en tres provincias del país. El instrumento mide dimensiones como reacción, aprendizaje percibido y aplicabilidad de la capacitación, permitiendo establecer asociaciones entre la formación recibida y la adopción de prácticas seguras (uso de contraseñas robustas, autenticación multifactor, actualización de sistemas) así como la frecuencia de reportes de incidentes.

El alcance del proyecto incluye la identificación de barreras que limitan la efectividad de los programas formativos, tales como la sobrecarga laboral, la conectividad deficiente y la falta de recursos tecnológicos. Asimismo, el estudio genera evidencia que contribuya al diseño de políticas públicas y estrategias institucionales orientadas a fortalecer la ciberseguridad en el sistema sanitario ecuatoriano.

La relevancia del proyecto radica en su aporte social, profesional y científico: socialmente, busca proteger los datos sensibles de los pacientes; profesionalmente, ofrece lineamientos para mejorar la gestión de la seguridad en instituciones de salud; y científicamente, llena un vacío en la literatura nacional sobre el impacto de la capacitación en ciberseguridad en entornos vulnerables.

En síntesis, este proyecto evalúa la efectividad de la formación en ciberseguridad y propone recomendaciones prácticas y políticas que fortalezcan la resiliencia digital del sector salud en Ecuador, contribuyendo a la protección de la información y a la mejora de la confianza institucional frente a las amenazas cibernéticas.

1.3 OBJETIVOS DEL PROYECTO

1.3.1 OBJETIVO GENERAL

Analizar la relación entre la capacitación en ciberseguridad y la adopción de prácticas seguras, así como la frecuencia de reportes de vulnerabilidades en centros de salud rurales y hospitales públicos del Ecuador, con el fin de generar evidencia empírica que contribuya al fortalecimiento de la seguridad digital en el sistema sanitario.

1.3.2 OBJETIVOS ESPECÍFICOS

1. Comparar el nivel de cumplimiento de prácticas seguras (porcentaje de uso de contraseñas robustas, MFA, actualización de sistemas) entre instituciones que han recibido capacitación y aquellas que no.

2. Identificar las principales barreras (tiempo, recursos tecnológicos, conectividad) que limitan la implementación efectiva de cursos virtuales y campañas internas, mediante análisis de frecuencia y correlación con variables demográficas.

3. Medir la percepción del personal de salud sobre la utilidad y efectividad de la capacitación en ciberseguridad, utilizando una escala Likert (1–5) en dimensiones de satisfacción, aplicabilidad y confianza en la reducción de riesgos.

1.4 JUSTIFICACIÓN DEL PROYECTO

La digitalización del sector salud en Ecuador ha generado una creciente dependencia de sistemas informáticos para la gestión de datos clínicos y administrativos. Si bien esta transformación ha mejorado la eficiencia y el acceso a la información, también ha incrementado la exposición a riesgos cibernéticos, especialmente en hospitales públicos y centros rurales con infraestructura limitada. En este contexto, la **capacitación en ciberseguridad** se presenta como una herramienta estratégica para mitigar vulnerabilidades, fortalecer la cultura de seguridad digital y fomentar el reporte oportuno de incidentes.

La relevancia del proyecto se fundamenta en varios ámbitos:

Social: contribuye a la protección de datos sensibles de pacientes, garantizando la confidencialidad y confianza en los servicios de salud.

Profesional: ofrece lineamientos prácticos para mejorar la gestión institucional y la resiliencia digital en entornos vulnerables.

Científico: aporta evidencia empírica en un campo poco explorado en el contexto ecuatoriano, cerrando brechas en la literatura sobre el impacto de la formación en ciberseguridad en el sector sanitario.

Además, los resultados facilitan la formulación de propuestas y la identificación de factores que inciden en la efectividad de los programas formativos, así como el diseño de políticas públicas orientadas a fortalecer la seguridad digital del sistema sanitario. De esta manera, el proyecto no solo busca evaluar la relación entre capacitación y prácticas seguras, sino también plantear soluciones aplicables y sostenibles que contribuyan al desarrollo de una cultura de ciberseguridad en instituciones de salud pública.

1.5 ALCANCE DEL PROYECTO

El proyecto se desarrolla en el contexto del sistema de salud público ecuatoriano, con énfasis en hospitales públicos y centros de salud rurales de las provincias de Guayas, Manabí y Los Ríos. Estas provincias se seleccionan por su diversidad geográfica, sus distintos niveles de infraestructura tecnológica y la presencia —o ausencia— de experiencias previas en programas de capacitación en ciberseguridad.

El alcance del estudio se delimita de la siguiente manera:

- **Dimensión temática:** se analiza la relación entre la capacitación en ciberseguridad y dos variables dependientes: la adopción de prácticas seguras y la frecuencia de reportes de vulnerabilidades.
- **Dimensión poblacional:** se incluye a 50 profesionales de salud del ámbito administrativo y técnico, seleccionados mediante una muestra estratificada de carácter exploratorio, con el fin de equilibrar la distribución territorial de la muestra.

- **Dimensión temporal:** se aplica un diseño transversal, con recolección de datos en un único momento, lo que permite caracterizar el estado actual del fenómeno de estudio.
- **Dimensión metodológica:** se emplea un enfoque cuantitativo, no experimental y correlacional, mediante cuestionarios estructurados tipo Likert para medir reacción, aprendizaje percibido y aplicabilidad de la capacitación.
- **Dimensión práctica:** se evalúan prácticas de protección digital —contraseñas robustas, autenticación multifactor, actualización de sistemas y respaldo de datos—, así como la disposición del personal para reportar incidentes de seguridad.

En síntesis, el alcance del proyecto se limita a evaluar el impacto de la capacitación en ciberseguridad en una muestra exploratoria distribuida territorialmente de instituciones públicas de salud, sin extenderse a clínicas privadas ni a otros sectores. Sus hallazgos aportan evidencia inicial aplicable al contexto estudiado y adaptado a diferentes contextos del sistema sanitario ecuatoriano.

CAPÍTULO II: MARCO TEÓRICO Y METODOLOGÍA

1.6 MARCO TEÓRICO

2.1.1 Contextualización de la ciberseguridad en el sector salud

La digitalización acelerada de los servicios sanitarios ha ampliado la superficie de ataque y ha incrementado la criticidad de los incidentes, debido al alto valor de los datos clínicos y a la creciente dependencia operativa de los sistemas informáticos. En el contexto ecuatoriano, los hospitales públicos y los centros de salud rurales enfrentan limitaciones de infraestructura, presupuestos ajustados y escasez de personal especializado, condiciones que incrementan la exposición a amenazas como ransomware, phishing, malware y fallas asociadas al factor humano. Este escenario sustenta la necesidad de analizar la capacitación en ciberseguridad como un mecanismo para fortalecer prácticas seguras y consolidar una cultura organizacional de seguridad.

En este marco, el problema de estudio se sitúa en instituciones públicas y rurales, y se plantea que la formación del personal influye en la implementación de medidas de protección específicas, tales como el uso de contraseñas robustas, la autenticación multifactor, la actualización oportuna de sistemas y la disposición para reportar vulnerabilidades. Estos elementos orientan el desarrollo del marco teórico hacia enfoques que vinculan la educación con cambios conductuales observables y con resultados organizacionales susceptibles de medición.

2.1.2 Modelos de evaluación del impacto formativo

• ***Modelo de Kirkpatrick (niveles 1 a 4).*** Este modelo evalúa la capacitación en cuatro niveles: reacción (satisfacción), aprendizaje (conocimientos y habilidades adquiridas), comportamiento (transferencia al puesto) y resultados (impacto organizacional). Para el presente estudio, el nivel 3 es clave porque vincula la formación con prácticas seguras —por ejemplo, el uso de MFA o la detección de phishing— y el nivel 4 permite observar efectos en indicadores como la disminución de incidentes o el aumento de reportes voluntarios.

• ***Extensión de Phillips (ROI).*** La adición del nivel 5 por (Phillips & Phillips, 2016)

introduce la estimación del retorno de la inversión, aspecto especialmente relevante en instituciones con recursos limitados. Aun cuando el alcance del estudio es correlacional y transversal, este marco incorpora métricas económicas complementarias (p. ej., costos evitados por incidentes) que pueden integrarse en evaluaciones de seguimiento. La adopción de estos modelos asegura coherencia entre los objetivos (medir la relación entre capacitación y prácticas/ reportes) y los indicadores de resultado, articulando una cadena lógica desde la exposición formativa hasta los cambios conductuales y organizacionales.

2.1.3 Teorías psicosociales para explicar el cambio de conducta en seguridad

• ***Teoría del Comportamiento Planeado (TPB) de*** (Ajzen, 1991). Propone que el comportamiento está determinado por las actitudes, las normas subjetivas y el control conductual percibido. En el ámbito sanitario, la capacitación puede modificar actitudes (valorar la seguridad), influir en normas (expectativas del equipo y de la institución) y aumentar el control percibido (autoeficacia para aplicar medidas), favoreciendo prácticas seguras sostenibles.

• ***Modelos de concienciación en seguridad (Security Awareness Model).*** Distinguen conocimiento, actitud y comportamiento, subrayando que el éxito de la concienciación no se limita a transmitir información, sino a provocar cambios medibles en hábitos cotidianos (bloqueo de sesión, actualización oportuna, respaldo de datos, reporte ágil).

• ***Motivación de protección y economía del comportamiento***. Como marcos complementarios, ayudan a entender por qué el personal adopta —o no— prácticas seguras frente a costos percibidos (tiempo, fricción) y sesgos (exceso de confianza, normalización del riesgo). La capacitación efectiva reduce fricciones, provee atajos seguros (p. ej., gestores de contraseñas) y refuerza normas de equipo.

2.1.4 Estándares, marcos y buenas prácticas aplicables al sector salud

Para traducir la capacitación en prácticas observables, son útiles los marcos de gestión del riesgo y de control. En el contexto hospitalario, los contenidos formativos suelen alinearse con: (a) gestión de identidades y accesos (contraseñas, MFA, privilegios mínimos); (b) higiene digital básica (parcheo, actualizaciones, copias de seguridad); (c) protección del correo y navegación (phishing, adjuntos y enlaces); (d) manejo de datos sensibles (confidencialidad, integridad, disponibilidad) y (e) reporte y respuesta ante

incidentes. La estandarización de estas prácticas facilita la medición y la auditoría interna. En instituciones con capacidades heterogéneas —como centros rurales—, las guías de mínimos viables de seguridad y campañas de bajo costo (recordatorios, simulaciones de phishing, cartelería) complementan los cursos virtuales, mitigando barreras de acceso tecnológico y sobrecarga laboral.

2.1.5 Evidencia empírica previa sobre capacitación en ciberseguridad en salud

El presente estudio compila estudios internacionales que muestran reducciones significativas en clics de phishing y aumentos en reportes voluntarios tras programas de formación, pero también identifica barreras en América Latina: baja completitud de cursos por limitaciones de tiempo, conectividad y dispositivos; brecha entre conocimiento teórico y aplicación práctica; y disminución del efecto sin refuerzo periódico. Esta evidencia justifica diseños que combinen modalidades (e-learning, simulaciones, microrecordatorios) y evalúen resultados conductuales objetivos.

En el contexto ecuatoriano, se reconoce una brecha en literatura sobre el impacto real de la capacitación en instituciones públicas de salud. El presente estudio busca aportar datos correlacionales que orienten políticas y programas adaptados al país, considerando diversidad geográfica y niveles de infraestructura.

2.1.6 Constructos y variables del estudio

• Variable independiente: Capacitación en ciberseguridad. Incluye exposición a cursos virtuales, campañas internas y simulaciones. Dimensiones evaluadas: reacción, aprendizaje percibido y aplicabilidad.

• ***Variables dependientes***:

- Adopción de prácticas seguras;
- Frecuencia de reportes de vulnerabilidades.

• ***Indicadores conductuales de prácticas seguras:*** uso de contraseñas robustas (>=12 caracteres y combinación alfanumérica), habilitación de MFA, frecuencia de actualización de sistemas, reconocimiento de correos de phishing en simulaciones, respaldo periódico de datos, bloqueo de sesión al ausentarse, cumplimiento de políticas de privacidad y tiempo de respuesta a alertas.

• ***Indicadores de reporte:*** número de reportes voluntarios, canales utilizados, tiempo transcurrido entre detección y notificación.

La operacionalización propuesta permite observar el paso del aprendizaje a la acción y, eventualmente, al resultado organizacional.

2.1.7 Supuestos teóricos y proposiciones derivadas

De la integración de los modelos y teorías se derivan varias proposiciones:

(P1) La participación en programas de capacitación se asocia positivamente con mayores niveles de adopción de prácticas seguras medibles.

(P2) La capacitación con refuerzos periódicos y componentes prácticos se asocia con mayores tasas de reporte de incidentes frente a capacitaciones puntuales y exclusivamente teóricas.

(P3) El efecto de la capacitación está mediado por actitudes, normas y autoeficacia (TPB), y moderado por barreras contextuales (infraestructura, tiempo disponible).

(P4) En entornos con restricciones, intervenciones de bajo costo pero frecuentes (simulaciones de phishing, recordatorios) sostienen mejor el cambio conductual que cursos únicos extensos.

2.1.8 Implicaciones para el diseño de la capacitación y la medición

A partir del marco teórico, el diseño formativo se estructura en :

(a) conectar amenazas prevalentes del entorno con tareas reales del personal;

(b) incluir prácticas guiadas y simulaciones;

(c) reducir fricción para la conducta segura (p. ej., plantillas de contraseñas, instructivos de MFA);

(d) incorporar refuerzos periódicos;

(e) facilitar el reporte con canales simples.

En la medición, se recomienda triangulación: auto-reporte (escalas Likert de reacción y aplicabilidad), métricas objetivas (resultados de simulaciones, registros de activación de MFA), y datos de proceso (tasa de completitud de cursos). El enfoque correlacional y

transversal permite estimar asociaciones y generar hipótesis para estudios longitudinales o cuasiexperimentales futuros.

2.1.9 Síntesis integradora

El marco teórico vincula la capacitación con cambios conductuales y resultados organizacionales a través de modelos de evaluación (Kirkpatrick/Phillips) y teorías psicosociales (TPB, concienciación). En el sistema de salud público ecuatoriano, la efectividad depende de ajustar contenidos y formatos a las limitaciones locales y de medir indicadores que reflejen el trabajo cotidiano. Este andamiaje sustenta el análisis estadístico de la asociación entre capacitación y prácticas seguras/reportes, aportando evidencia útil para la formulación de políticas y programas formativos.

2.1.10 Enfoques contemporáneos de gestión del riesgo humano

Además de los modelos clásicos de evaluación formativa y las teorías psicosociales revisadas, la literatura reciente en ciberseguridad ha desarrollado enfoques específicamente orientados a gestionar el riesgo que representa el comportamiento humano dentro de las organizaciones.

El marco de referencia más utilizado a nivel internacional, el NIST Cybersecurity Framework, fue actualizado en su versión 2.0 en febrero de 2024. La actualización incorporó una sexta función central, denominada Govern (Gobernanza), que sitúa la supervisión y la asignación de responsabilidades sobre el riesgo de ciberseguridad — incluido el riesgo asociado al factor humano — como una función estratégica al mismo nivel que identificar, proteger, detectar, responder y recuperar (National Institute of Standards and Technology [NIST], 2024). Este cambio es relevante para el presente estudio porque reconoce explícitamente que la capacitación del personal no es una actividad aislada, sino parte de un sistema de gobernanza que debe medirse y reportarse a nivel institucional.

Relacionado con lo anterior, el modelo de arquitectura Zero Trust (confianza cero), formalizado por el NIST en la publicación especial SP 800-207, propone que ningún usuario o dispositivo debe considerarse confiable por defecto, incluso dentro de la red institucional, y que el acceso a los sistemas debe verificarse de forma continua (Rose et al., 2020). Aplicado al factor humano, este principio traduce la capacitación en verificación constante de identidad (autenticación multifactor), privilegios mínimos por

rol y monitoreo continuo del comportamiento, en lugar de depender únicamente de que el personal recuerde buenas prácticas después de un curso puntual.

Por otra parte, ha emergido en la industria y en la investigación reciente el concepto de Human Risk Management (HRM, gestión del riesgo humano) como una evolución de los programas tradicionales de concienciación (Security Awareness and Training). A diferencia de estos últimos, que se centran en la transmisión de contenidos y en tasas de finalización de cursos, el HRM propone un enfoque basado en datos de comportamiento real (por ejemplo, tasas de clic en simulaciones de phishing, activación de MFA o tiempo de respuesta ante alertas), con el fin de dirigir intervenciones personalizadas hacia el personal de mayor riesgo (Nurse et al., 2025). Estudios recientes muestran además que los programas de concienciación tradicionales tienen efectos positivos pero modestos y frecuentemente decrecientes con el tiempo si no se refuerzan periódicamente (Prümmer et al., 2025), lo cual es coherente con la evidencia empírica revisada en la sección 2.1.5 sobre la disminución del efecto formativo sin refuerzo.

Finalmente, el Security Awareness Maturity Model, desarrollado por el SANS Institute, ofrece una escala de cinco niveles para diagnosticar qué tan desarrollado está un programa de concienciación en una institución: desde la ausencia total de programa, pasando por un enfoque centrado únicamente en el cumplimiento normativo, hasta programas que logran un cambio sostenido de comportamiento y cuentan con métricas de impacto (SANS Institute, 2024). Este modelo es útil para el presente estudio porque permite ubicar a las instituciones de salud pública ecuatorianas analizadas dentro de una escala reconocida internacionalmente, y sugiere que el tránsito de capacitaciones puntuales (nivel de cumplimiento) hacia programas sostenidos con métricas (niveles superiores) podría explicar parte de la diferencia observada entre el Grupo A y el Grupo B.

En conjunto, estos cuatro enfoques —gobernanza (NIST CSF 2.0), verificación continua (Zero Trust), gestión de riesgo basada en datos (HRM) y maduración progresiva del programa (SANS SAMM)— amplían el marco teórico clásico de Kirkpatrick, Phillips y la Teoría del Comportamiento Planeado, situando la capacitación en ciberseguridad no como un evento aislado, sino como un componente de un sistema de gestión de riesgo humano en constante evolución.

1.7 METODOLOGÍA DEL PROYECTO

Para el análisis comparativo, la muestra se organiza en dos grupos definidos en función de la variable independiente "capacitación en ciberseguridad": el Grupo A (con capacitación) agrupa a quienes han recibido formación previa, y el Grupo B (sin capacitación) a quienes no la han recibido. Esta clasificación permite evaluar diferencias en la adopción de prácticas seguras y en la frecuencia de reporte de incidentes mediante análisis estadístico comparativo.

1.7.1 Enfoque, tipo y diseño

La investigación se enmarca en un enfoque cuantitativo, pues busca medir y analizar relaciones entre variables mediante datos numéricos y técnicas estadísticas. Es de tipo diagnóstico y correlacional, orientada a identificar el nivel de adopción de prácticas seguras y la frecuencia de reportes de vulnerabilidades en función de la capacitación recibida.

El alcance es correlacional: se busca establecer asociaciones entre la capacitación en ciberseguridad (variable independiente) y dos variables dependientes: la adopción de prácticas seguras (uso de contraseñas robustas, MFA, actualización de sistemas) y la frecuencia de reportes de vulnerabilidades.

El diseño es no experimental, transversal: se observan los fenómenos en su contexto natural, sin manipular variables, y la recolección de datos se realiza en un único momento temporal.

1.7.2 Fundamento teórico y método

El estudio se sustenta en el modelo de evaluación de impacto educativo de Kirkpatrick y Kirkpatrick (2006) y en la Teoría del Comportamiento Planeado (Ajzen, 1991), que vinculan la capacitación con cambios en actitudes, percepciones y comportamientos. También se considera el Security Awareness Model (Parsons et al., 2017).

El método es hipotético-deductivo: parte de hipótesis sobre el impacto de la capacitación y las verifica mediante análisis estadístico.

1.7.3 Grupos poblacionales y muestra

La población objetivo está conformada por personal administrativo y técnico de centros de salud rurales y hospitales públicos en tres provincias representativas del sistema sanitario ecuatoriano: Guayas, Manabí y Los Ríos. Estos grupos son relevantes por su exposición directa a sistemas informáticos y datos sensibles, y por ser destinatarios de programas de capacitación en ciberseguridad.

El tamaño muestral de 50 participantes, distribuidos por provincia y tipo de institución, se justifica por el carácter exploratorio y aplicado del estudio. Esta muestra estratificada permite comparar los dos grupos de análisis, identificar tendencias iniciales y estimar asociaciones entre la capacitación, la adopción de prácticas seguras y el reporte de incidentes. Los resultados no pretenden generalizarse a la totalidad del sistema sanitario ecuatoriano, sino aportar evidencia inicial para orientar futuras investigaciones y programas formativos.

1.8 METODOLOGÍA DE INVESTIGACIÓN

La investigación se enmarca en un enfoque cuantitativo, dado que busca medir y analizar relaciones entre variables mediante datos numéricos y técnicas estadísticas. El diseño adoptado es no experimental, correlacional y transversal, ya que no se manipulan variables independientes y la recolección de datos se realiza en un único momento temporal.

Tipo de investigación: Diagnóstica y correlacional. Se propone identificar el nivel de adopción de prácticas seguras y la frecuencia de reportes de vulnerabilidades en función de la capacitación recibida.

Alcance: Correlacional, porque se busca establecer asociaciones entre la capacitación en ciberseguridad (variable independiente) y dos variables dependientes:

Adopción de prácticas seguras (uso de contraseñas robustas, MFA, actualización de sistemas).

Frecuencia de reportes de vulnerabilidades.

Diseño: No experimental, transversal, observando el fenómeno en su contexto natural sin manipulación de variables.

Fundamento teórico: Se sustenta en el modelo de evaluación de impacto educativo de (Kirkpatrick & Kirkpatrick, 2006) y en la Teoría del Comportamiento Planeado (Ajzen, 1991), que vinculan la capacitación con cambios en actitudes, percepciones y comportamientos. También se considera el Security Awareness Model (Parsons et al., 2017)

Método: Hipotético-deductivo, partiendo de hipótesis sobre el impacto de la capacitación y verificándolas mediante análisis estadístico.

Grupos poblacionales involucrados La población objetivo está compuesta por personal administrativo y técnico de centros de salud rurales y hospitales públicos en tres provincias del Ecuador: Guayas, Manabí y Los Ríos. Estos grupos son relevantes por su exposición directa a sistemas digitales y por ser destinatarios de programas de capacitación en ciberseguridad.

Muestra: El tamaño muestral de 50 participantes se justifica por el carácter exploratorio y aplicado del estudio. Esta muestra estratificada de carácter exploratorio permite comparar dos grupos de análisis, identificar tendencias iniciales y estimar asociaciones entre la capacitación en ciberseguridad, la adopción de prácticas seguras y el reporte de incidentes. Los resultados no pretenden generalizarse a la totalidad del sistema sanitario ecuatoriano, sino aportar evidencia inicial para orientar futuras investigaciones y programas formativos.

1.9 TÉCNICAS DE RECOLECCIÓN DE INFORMACIÓN

Con el propósito de garantizar la validez, confiabilidad, consistencia interna y trazabilidad de los datos empíricos, la presente investigación integra un conjunto de procedimientos estandarizados de recolección, codificación, tabulación, depuración y análisis estadístico. Dichos procedimientos están orientados a examinar de manera rigurosa la relación existente entre la **capacitación en ciberseguridad** y: (i) la **adopción de prácticas seguras de seguridad de la información**, y (ii) la **frecuencia de reporte de vulnerabilidades e incidentes**, en el contexto del **sistema de salud pública del Ecuador**.

El enfoque metodológico responde a un **diseño cuantitativo, correlacional y transversal**, adecuado para identificar asociaciones significativas entre variables medidas en un único momento temporal, sin manipulación experimental.

1.9.1 1. Hipótesis de investigación

Hipótesis principales

- **H1:** La capacitación en ciberseguridad se asocia de manera significativa con una mayor adopción de prácticas seguras por parte del personal del sistema de salud pública.
- **H2:** La capacitación en ciberseguridad se asocia de manera significativa con una mayor frecuencia de reporte de vulnerabilidades e incidentes de seguridad.

Estas hipótesis parten del supuesto teórico de que la formación estructurada y recurrente en ciberseguridad influye positivamente en el **comportamiento seguro del usuario** y en su **participación activa en la gestión de incidentes**.

Hipótesis complementarias (por dimensiones formativas)

Con el fin de analizar los **mecanismos internos de la capacitación**, se plantean hipótesis adicionales alineadas con modelos de evaluación de la formación (reacción–aprendizaje–transferencia):

- **H3:** La aplicabilidad percibida de la capacitación se asocia de manera significativa con la adopción de prácticas seguras.
- **H4:** La aplicabilidad percibida de la capacitación se asocia de manera significativa con la frecuencia de reporte de vulnerabilidades e incidentes.
- **H5:** El aprendizaje percibido derivado de la capacitación se asocia de manera significativa con la adopción de prácticas seguras.
- **H6:** La reacción frente a la capacitación se asocia de manera significativa tanto con el aprendizaje percibido como con la aplicabilidad de los contenidos formativos.

Para cada una de las hipótesis planteadas se formula su correspondiente **hipótesis nula (H0)**, que establece la inexistencia de asociación estadísticamente significativa entre las variables analizadas.

1.9.2 2. Técnica e instrumento de recolección de datos

Instrumento principal: cuestionario estructurado

La recolección de datos se realiza mediante un **cuestionario estructurado**, diseñado específicamente para el estudio y compuesto por **ítems cerrados** medidos en una **escala tipo Likert de cinco puntos (1–5)**, donde valores mayores indican mayor nivel de acuerdo, frecuencia o presencia del atributo evaluado.

El instrumento permite medir las siguientes variables y dimensiones:

- **Capacitación en ciberseguridad**: nivel de exposición e intensidad formativa, considerando cursos formales, campañas internas, simulaciones, frecuencia de capacitación y cobertura temática.
- **Resultados de la capacitación**:
    - *Reacción*: percepción general, utilidad y satisfacción con la capacitación recibida.
    - *Aprendizaje percibido*: autovaloración del conocimiento y habilidades adquiridas.
    - *Aplicabilidad*: grado de transferencia de los conocimientos al puesto de trabajo.
- **Prácticas seguras de ciberseguridad**: uso de contraseñas robustas, autenticación multifactor (MFA), actualización de sistemas, copias de seguridad, y reconocimiento de intentos de phishing.
- **Reporte de vulnerabilidades/incidentes**: frecuencia de reporte, disposición a reportar y conocimiento de los canales institucionales.

Modalidad de aplicación

El cuestionario se aplica mediante una **plataforma digital segura**, lo que permite:

- Garantizar el **anonimato de los participantes**.
- Estandarizar el proceso de aplicación.

- Reducir errores de digitación.
- Registrar de forma homogénea y automática las respuestas.
- Facilitar la exportación de datos para su análisis estadístico.

1.9.3 Pilotaje, validez y confiabilidad del instrumento

Pilotaje del cuestionario

Previo a la aplicación definitiva, el instrumento se somete a un **pilotaje con 20 participantes**, con el objetivo de evaluar:

- Claridad semántica y comprensión de los ítems.
- Coherencia interna de las dimensiones.
- Tiempo promedio de respuesta.
- Identificación de ambigüedades o redundancias.

Los participantes del pilotaje no fueron incorporados al análisis estadístico final, con el propósito de evitar sesgos derivados de la familiarización previa con el instrumento y garantizar la independencia de la muestra definitiva.

Confiabilidad

El Índice de Prácticas Seguras (IPS) se construye como un índice compuesto aditivo integrado por siete comportamientos independientes de ciberseguridad. Debido a que estos indicadores representan prácticas distintas y no una única dimensión psicológica latente, el coeficiente alfa de Cronbach no se utiliza como criterio principal de validación del índice. El valor obtenido se reporta únicamente como referencia complementaria en los anexos, junto con el procedimiento de cálculo y la evidencia de reproducibilidad.

Validez de contenido

La **validez de contenido** se sustenta mediante una revisión técnica de la alineación entre:

- Variables de estudio.

- Dimensiones analíticas.
- Indicadores operativos.
- Ítems del cuestionario.

Este proceso se apoya en literatura especializada sobre **formación en ciberseguridad, comportamiento del usuario y gestión de incidentes**, asegurando coherencia teórica y metodológica.

Los procedimientos estadísticos, el cálculo del IPS, la estimación de indicadores de asociación y la verificación de reproducibilidad se documentan en los anexos metodológicos y estadísticos correspondientes.

1.9.4 4. Muestreo y control de sesgos

Diseño muestral

Se emplea **una muestra estratificada de carácter exploratorio**, considerando como criterios de estratificación:

- **Provincia**, para asegurar equilibrio territorial de la muestra.
- **Rol funcional**, para capturar diferencias entre perfiles técnicos, administrativos y asistenciales.

A. Ampliación del deseño muestral

Este enfoque permite mejorar la precisión de las estimaciones y la identificación de patrones en la muestra analizada.

Los criterios de inclusión consideraron a personal administrativo y técnico con acceso directo a sistemas informáticos institucionales y una antigüedad mínima de seis meses en el puesto, con el fin de asegurar familiaridad con las herramientas digitales evaluadas. Se excluyó al personal en período de inducción y a quienes no tuvieran acceso a un equipo informático propio dentro de su función. El contacto con las instituciones participantes se realizó a través de las jefaturas de talento humano y de tecnología de cada centro de salud, quienes facilitaron la difusión de la encuesta entre el personal elegible. La asignación al Grupo A (con capacitación) o al Grupo B (sin capacitación) no fue aleatoria, sino observacional: se clasificó a cada participante según si había recibido o no capacitación

formal en ciberseguridad en los doce meses previos a la aplicación del instrumento, de acuerdo con su propia declaración en la Sección 1 del cuestionario.

Control de sesgos

- **Sesgo de selección**: mitigado mediante una muestra estratificada de carácter exploratorio y criterios de inclusión claramente definidos.
- **Sesgo de realización (respuesta)**: controlado mediante instrucciones uniformes, tiempos definidos y aplicación digital.
- **Sesgo de deseabilidad social**: reducido a través del anonimato, la ausencia de identificación personal y la formulación neutral de los ítems.

B. Resumen de limitaciones metodológicas

Es importante advertir, desde esta etapa metodológica, que el estudio presenta limitaciones que condicionan el alcance de sus resultados. La muestra de 50 participantes, obtenida mediante muestreo estratificado de carácter exploratorio y no probabilístico, no permite generalizar los hallazgos a la totalidad del sistema de salud pública ecuatoriano. Asimismo, el diseño transversal permite identificar asociaciones entre variables, pero no establecer relaciones de causalidad entre la capacitación y las prácticas seguras observadas. El desarrollo completo de estas limitaciones, incluyendo las relativas al Índice de Prácticas Seguras como medida aditiva, se presenta en el apartado 'Limitaciones del estudio' del Capítulo III (p. 61).

1.9.5 5. Tabulación, codificación y depuración de datos

Codificación

- Las respuestas en escala Likert se codifican numéricamente de **1 a 5**.
- Los ítems formulados en sentido inverso (si existen) se **recodifican** para mantener una dirección consistente, donde valores mayores indican mayor nivel del constructo evaluado.

Construcción de índices compuestos

Se calculan **puntajes por dimensión** mediante el promedio (o suma estandarizada) de los ítems correspondientes:

- **Cap_Expo**: exposición e intensidad de capacitación.
- **Reaccion**, **Aprendizaje**, **Aplicabilidad**.
- **Practicas_Total**, con subíndices por tipo de control de seguridad.
- **Reporte_Frec**, como variable ordinal o índice compuesto según el número de ítems.

Depuración y control de calidad

- Verificación de rangos válidos (1–5).
- Identificación de duplicados.
- Análisis de consistencia lógica entre respuestas.
- Reporte de valores faltantes por ítem y por participante.

Criterios de integridad de datos:

- Exclusión del análisis inferencial de sujetos con **más del 20 % de ítems faltantes**.
- Tratamiento de faltantes residuales mediante **imputación por media del sujeto dentro de la dimensión**, siempre que sea metodológicamente justificable y debidamente documentado.

CAPÍTULO III: RESULTADOS Y ANÁLISIS

1.10 RECOLECCIÓN Y TABULACIÓN

Los resultados se presentan en función de dos grupos de análisis: Grupo A (con capacitación), conformado por profesionales de salud con capacitación en ciberseguridad, y Grupo B (sin capacitación) , conformado por profesionales de salud sin capacitación en ciberseguridad.

Herramientas:

- La tabulación y análisis se ejecutan con software estadístico (p. ej., SPSS, R o Python), garantizando reproducibilidad.

Operacionalización de variables e indicadores

Escala base: Likert 1–5 (1 = totalmente en desacuerdo / nunca; 5 = totalmente de acuerdo / siempre, según el ítem).

Cálculo: índices por dimensión mediante promedios (o sumas estandarizadas).

La siguiente tabla presenta la operacionalización de las variables del estudio, detallando las dimensiones analíticas, los indicadores observables y la escala de medición correspondiente. La variable independiente corresponde a la capacitación en ciberseguridad, mientras que las variables dependientes son la adopción de prácticas seguras y la frecuencia de reporte de vulnerabilidades.

Se recopila información estructurada y sistemática mediante un cuestionario validado aplicado a 50 profesionales de salud pública en tres provincias del Ecuador (Guayas, Manabí y Los Ríos.

1.11 TABLA 1. OPERACIONALIZACIÓN DE VARIABLES, DIMENSIONES, INDICADORES Y MEDICIÓN

Variable	Tipo	Dimensión	Indicadores	Escala de Medición
Capacitación en Ciberseguridad	Independiente	Exposición formativa	• Cursos virtuales completados • Campañas internas • Simulaciones de phishing • Frecuencia de capacitación • Cobertura temática	Escala dicotómica (0=Sin cap., 1=Con cap.) / Escala Likert 1–5
		Reacción (Kirkpatrick N1)	• Satisfacción con la capacitación • Utilidad percibida • Valoración general del programa	Escala Likert 1–5 (1=Muy insatisfecho, 5=Muy satisfecho)
		Aprendizaje percibido (Kirkpatrick N2)	• Autoevaluación de conocimientos • Habilidades adquiridas • Comprensión de amenazas	Escala Likert 1–5
		Aplicabilidad (Kirkpatrick N3)	• Transferencia al puesto • Uso real de conocimientos • Autoeficacia (TPB)	Escala Likert 1–5 (índice promedio)
Adopción de Prácticas Seguras	Dependiente	Gestión de accesos	• Uso de contraseñas robustas (≥12 caracteres) • Habilitación de autenticación multifactor (MFA) • Bloqueo de sesión al ausentarse	Dicotómica (0=No / 1=Sí); índice compuesto 0–7
		Higiene digital	• Actualización periódica de sistemas • Respaldo de datos • Reconocimiento de phishing	Dicotómica (0=No / 1=Sí)
		Protección de datos	• Cumplimiento de políticas de privacidad • Manejo de información sensible	Dicotómica (0=No / 1=Sí)
Frecuencia de Reporte	Dependiente	Reporte de vulnerabilidades	• Número de reportes voluntarios • Canales institucionales utilizados • Tiempo detección–notificación • Disposición a reportar	Dicotómica (0=No reporta / 1=Sí reporta) o escala ordinal 1–5

Variable	Tipo	Dimensión	Indicadores	Escala de Medición
Variables de Control / Covariables	Control	Características sociodemográficas	• Provincia (Guayas, Manabí, Los Ríos) • Tipo de institución (Hospital Público / C. Salud Rural) • Rol funcional (Administrativo / Técnico / Asistencial)	Nominal (código provincia/institución/rol)

Nota: La escala Likert 1–5 se utiliza para dimensiones de reacción, aprendizaje y aplicabilidad. Las variables de prácticas seguras se codifican como dicotómicas (0/1) y se agrupan en el Índice de Prácticas Seguras (0–7).

1.12 Justificación metodológica

Grupo	Descripción	n
Grupo A (con capacitación)	Personal que recibe capacitación en ciberseguridad	25
Grupo B (sin capacitación)	Personal que NO recibe capacitación	25
TOTAL	**Muestra completa — 3 provincias**	**50**

Tabla 1.1 — Estructura del diseño comparativo de grupos equivalentes.

La comparación entre grupos permite identificar diferencias asociadas a la capacitación, sin asumir causalidad ni equivalencia con diseños pre-post.

1.13 Tabla 1.2 — Distribución de la muestra por provincia y tipo de institución.

Provincia	Grupo A (Con capacitación.)	Grupo B (Sin capacitación.)	Total
Guayas	8 (32%)	9 (36%)	17
Manabí	9 (36%)	8 (32%)	17

Provincia	Grupo A (Con capacitación.)	Grupo B (Sin capacitación.)	Total
Los Ríos	8 (32%)	8 (32%)	16
Hospital Público	14 (56%)	13 (52%)	27
Centro de Salud Rural	11 (44%)	12 (48%)	23
TOTAL	**25 (100%)**	**25 (100%)**	**50**

La siguiente tabla presenta la correspondencia entre los objetivos específicos de la investigación, las técnicas estadísticas aplicadas y los resultados y su análisis.

1.14 Tabla 2. Matriz de Objetivos, Técnicas de Análisis y Salidas Esperadas

N°	Objetivo Específico	Hipótesis Asociada	Técnica Estadística	Salida Esperada	Herramienta
1	Comparar el cumplimiento de prácticas seguras entre grupos con y sin capacitación (contraseñas, MFA, actualización)	H1: La capacitación se asocia con mayor adopción de prácticas seguras	Chi-cuadrado de independencia; Prueba t de Student para índice compuesto; Estadísticos descriptivos (media, DE)	Diferencia estadísticamente significativa en la proporción de adopción de prácticas seguras entre Grupo A (con capacitación.) y Grupo B (sin capacitación.)	Python / SPSS / R
2	Identificar barreras que limitan la capacitación (tiempo, recursos, conectividad) y su correlación con variables demográficas	H3/H5: Dimensiones formativas (aplicabilidad, aprendizaje) se asocian con prácticas seguras	Análisis de frecuencias; Correlación de Spearman (variables ordinales); Tablas de contingencia	Ranking de barreras identificadas; Coeficientes de correlación con significancia estadística	Python / SPSS
3	Medir la percepción del personal sobre	H6: Reacción se asocia con	Estadísticos descriptivos por	Índices por dimensión; Confiabilidad del	Python / R

N°	Objetivo Específico	Hipótesis Asociada	Técnica Estadística	Salida Esperada	Herramienta
	utilidad y efectividad de la capacitación mediante escala Likert (satisfacción, aplicabilidad, confianza)	aprendizaje y aplicabilidad	dimensión (media, mediana, DE); Alfa de Cronbach; Análisis de componentes por dimensión	instrumento (α); Perfil de percepción por provincia y tipo de institución	
4	Estimar la asociación entre capacitación y frecuencia de reporte de vulnerabilidades	H2/H4: Capacitación y aplicabilidad se asocian con reporte de incidentes	Chi-cuadrado; Regresión logística binaria (Reporte=0/1); OR e intervalos de confianza	Odds Ratio de reporte según grupo; p-valores; Modelo predictivo de reporte	Python / SPSS
5	Comparar indicadores entre provincias y tipos de institución	Análisis exploratorio / moderación contextual	ANOVA / Kruskal-Wallis; Tablas comparativas por estrato (provincia, rol)	Diferencias provinciales e institucionales en prácticas y reporte; Identificación de subgrupos prioritarios	Python / R

Nota: El nivel de significancia adoptado es α = 0.05. Para regresión logística se reportan OR, IC 95% y p-valor. La confiabilidad se evalúa con α de Cronbach

1.15 Resultados de la Aplicación de Medidas de Ciberseguridad tras la Capacitación

El análisis comparativo entre el Grupo A (con capacitación) y el Grupo B (sin capacitación) se observan diferencias favorables al Grupo A; algunas alcanzan significancia estadística. El personal formado presenta una conducta de seguridad digital consistentemente superior, evidenciando la asociación significativa entre capacitación y prácticas seguras de los programas de capacitación en ciberseguridad.

1.16 Comparación de indicadores de prácticas seguras (Grupo A con capacitación vs. Grupo B sin capacitación)

1.16.1 Tabla 2.1 — Prueba Chi-cuadrado de independencia por indicador. *** p<0.001; ** p<0.01; * p<0.05. n=50, gl=1, valor crítico=3.841.

Indicador de Seguridad	Grupo A (Con Capacitación.) %	Grupo B (Sin Capacitación.) %	Diferencia (pp)	χ^2 (gl=1)	p-valor	Decisión
Uso de Contraseñas Robustas	76.0%	56.0%	+20.0	2.228	0.136	No sig.
Habilitación de MFA	76.0%	36.0%	+40.0	8.117	0.004	** Sig.
Actualización de Sistemas	72.0%	60.0%	+12.0	0.802	0.370	No sig.
Reconocimiento de Phishing	72.0%	36.0%	+36.0	6.522	0.011	* Sig.
Bloqueo de Sesión	72.0%	60.0%	+12.0	0.802	0.370	No sig.
Respaldo de Datos	60.0%	40.0%	+20.0	2.000	0.157	No sig.
Cumplimiento de Privacidad	84.0%	60.0%	+24.0	2.480	0.115	No sig.
Reporte de Incidentes	84.0%	32.0%	+52.0	13.875	< 0.001	*** Sig.

Los tres indicadores con diferencias estadísticamente significativas son:

1. Reporte de Incidentes: +52 pp (84% vs. 32%, χ^2=13.875, p<0.001) — asociación más fuerte observada en la muestra.
2. Habilitación de MFA: +40 pp (76% vs. 36%, χ^2=8.117, p=0.004) — tecnología de acceso seguro.
3. Reconocimiento de Phishing: +36 pp (72% vs. 36%, χ^2=6.522, p=0.011) — detección de amenazas.

1.17 Índice de Prácticas Seguras (IPS) — Estadísticos descriptivos por grupo

El Índice de Prácticas Seguras (IPS) es un índice compuesto que suma los 7 indicadores binarios de comportamiento seguro, con rango de 0 a 7. Permite comparar el nivel global de seguridad entre grupos de manera continua.

1.17.1 Tabla 2.2 — Estadísticos descriptivos del IPS por grupo.

Estadístico	Grupo A — Con Capacitación	Grupo B — Sin Capacitación
Media (promedio)	**5.12**	**3.20**
Mediana	5.0	3.0
Desviación Estándar	1.24	1.22
Mínimo	3	1
Máximo	7	5
Rango intercuartílico	4-6	2-4

Prueba t de Student para muestras independientes:

$t(48) = 5.518$ | $p < 0.000001$ | Diferencia: +1.92 puntos en IPS

Interpretación: El Grupo A (con capacitación) supera significativamente al Grupo B (sin capacitación) en el nivel global de prácticas de ciberseguridad. Se rechaza H0 de igualdad de medias ($\alpha = 0.05$).

1.18 IPS por provincia y tipo de institución

1.18.1 Tabla 2.3 — IPS promedio y tasa de reporte por provincia y tipo de institución.

Provincia / Institución	IPS — Grupo A(con capacitación)	IPS — Grupo B (sin capacitación)	Diferencia	Reporte A%	Reporte B%
Guayas	5.12	3.44	+1.68	87.5%	22.2%
Manabí	5.11	3.00	+2.11	77.8%	50.0%
Los Ríos	5.12	3.12	+2.00	87.5%	25.0%
Hospital Público	4.71	3.00	+1.71	85.7%	30.8%
Centro de Salud Rural	5.64	3.42	+2.22	81.8%	33.3%
TOTAL	**5.12**	**3.20**	**+1.92**	**84.0%**	**32.0%**

Las tres provincias muestran el mismo patrón de ventaja para el Grupo A (con capacitación), los resultados identifican que la asociación observada se mantiene en las diferencias geográficas e infraestructurales. La mayor diferencia se observa en los Centros de Salud Rural (diferencia IPS = +2.22), posiblemente porque este personal tiene menor exposición previa a prácticas de seguridad digital.

1.19 RESULTADOS DEL ANÁLISIS ESTADÍSTICO (n = 50)

La muestra está compuesta por 50 profesionales de salud distribuidos en tres provincias del Ecuador, con una muestra estratificada de carácter exploratorio. El Grupo A (con capacitación en ciberseguridad) cuenta con 25 participantes y el Grupo B (sin capacitación) con 25 participantes.

1.19.1 Tabla 3. Caracterización de la Muestra por Provincia, Tipo de Institución y Grupo

Estrato	Grupo A (Con Capacitación.) n	Grupo A (con capacitación) %	Grupo B (Sin Capacitación.) n	Grupo B (sin capacitación) %	Total n
Guayas	8	32.0%	9	36.0%	17
Manabí	9	36.0%	8	32.0%	17
Los Ríos	8	32.0%	8	32.0%	16
Hospital Público	14	56.0%	13	52.0%	27
Centro de Salud Rural	11	44.0%	12	48.0%	23
TOTAL	**25**	**100%**	**25**	**100%**	**50**

Nota: La distribución por tipo de institución refleja la composición del sistema de salud pública en las tres provincias. Grupos A y B balanceados (n=25 c/u).

1.20 Porcentaje de Uso de Contraseñas Seguras

El análisis del indicador de contraseñas robustas —definidas como aquellas con 12 o más caracteres, combinación alfanumérica y uso de símbolos especiales— constituye uno de los indicadores base de la higiene digital del personal sanitario.

1.21 Resultados globales y por segmento

1.21.1 Tabla 3.1 — Porcentaje de uso de contraseñas seguras por segmento (n=50).

Segmento	n	Usa Contraseñas Seguras	No Usa	Porcentaje Uso
TOTAL MUESTRA	50	33	17	66.0%

Segmento	n	Usa Contraseñas Seguras	No Usa	Porcentaje Uso
Grupo A — Con capacitación	25	19	6	76.0%
Grupo B — Sin capacitación	25	14	11	56.0%
Hospital Público	27	17	10	63.0%
Centro de Salud Rural	23	16	7	69.6%
Guayas	17	11	6	64.7%
Manabí	17	11	6	64.7%
Los Ríos	16	11	5	68.8%

HALLAZGOS CLAVE — Contraseñas Seguras

66% de la muestra total usa contraseñas robustas (33 de 50 participantes).

El personal capacitado (Grupo A) supera en 20 pp al no capacitado: 76% vs. 56%.

Correlación Spearman: rs = 0.211 (positiva, dirección correcta; p = 0.141, no significativa con n=50).

1.22 Interpretación del indicador

Aunque la diferencia de 20 puntos porcentuales entre grupos no alcanza significancia estadística formal ($\chi^2 = 2.228$, $p = 0.136$) con n=50, representa una tendencia clínicamente relevante. En el contexto de seguridad de la información hospitalaria, una diferencia de 20 pp en el uso de contraseñas robustas equivale a 5 usuarios adicionales por cada 25 que adoptan esta práctica de protección básica, lo que se traduce en una reducción directa de la superficie de ataque por credenciales débiles.

La correlación de Spearman entre capacitación y uso de contraseñas (rs = 0.211) indica una asociación positiva moderada-baja. Para investigaciones futuras con muestras de n ≥

150 (escala provincial), esta diferencia requiere una muestra más grande para evaluar con mayor potencia estadística.

La siguiente tabla presenta los estadísticos descriptivos del Índice de Prácticas Seguras (IPS) calculado como suma de los 7 indicadores binarios. Se reporta media, mediana y desviación estándar por grupo, junto con la confiabilidad del instrumento mediante el coeficiente alfa de Cronbach.

1.23 Tabla 4. Estadísticos Descriptivos por Dimensión y Confiabilidad del Instrumento (α de Cronbach)

Dimensión / Índice	Grupo A (con capacitación) Media	Grupo A (con capacitación) Mediana	Grupo A (con capacitación) DE	Grupo B (sin capacitación) Media	Grupo B (sin capacitación) Mediana	Grupo B (sin capacitación) DE	α Cronbach
Índice de Prácticas Seguras (IPS, 0–7)	**5.12**	**5.0**	**1.24**	**3.20**	**3.0**	**1.22**	**0.369**
Uso de contraseñas robustas	0.76	1.0	0.44	0.56	1.0	0.51	—
Habilitación de MFA	0.76	1.0	0.44	0.36	0.0	0.49	—
Actualización de sistemas	0.72	1.0	0.46	0.60	1.0	0.50	—
Reconocimiento de phishing	0.72	1.0	0.46	0.36	0.0	0.49	—
Bloqueo de sesión	0.72	1.0	0.46	0.60	1.0	0.50	—

Dimensión / Índice	Grupo A (con capacitación) Media	Grupo A (con capacitación) Mediana	Grupo A (con capacitación) DE	Grupo B (sin capacitación) Media	Grupo B (sin capacitación) Mediana	Grupo B (sin capacitación) DE	α Cronbach
Respaldo de datos	0.60	1.0	0.50	0.40	0.0	0.50	—
Cumplimiento de privacidad	0.84	1.0	0.37	0.60	1.0	0.50	—
Reporte de incidentes	0.84	1.0	0.37	0.32	0.0	0.48	—

Nota: DE = Desviación Estándar. El α de Cronbach global del IPS es 0.369,este valor no permite afirmar alta consistencia interna; se reporta como limitación, lo cual refleja la independencia relativa de los ítems conductuales binarios en una muestra pequeña (n=50). Para el análisis inferencial se utiliza el IPS como índice compuesto continuo (0–7).

La prueba t de Student para muestras independientes arroja un resultado estadísticamente significativo ($t = 5.518$, $p < 0.000001$), lo que indica que el Grupo A (con capacitación) presenta un índice de prácticas seguras significativamente más alto (Media = 5.12, DE = 1.24) comparado con el Grupo B (sin capacitación) (Media = 3.20, DE = 1.22).

1.24 Nivel de Capacitación Recibida

El nivel de capacitación se operacionalizó de dos formas complementarias: (a) como variable dicotómica —Grupo A=1 (con capacitación) / Grupo B=0 (sin capacitación)— y (b) como índice continuo a través del IPS, que refleja la transferencia conductual real del aprendizaje al puesto de trabajo.

1.25 Distribución y estadísticos del nivel de capacitación

1.25.1 Tabla 4.1 — Nivel de capacitación y transferencia conductual por dimensión y estrato. *** p<0.001; ** p<0.01; * p<0.05.

Dimensión	Grupo A (Con Capacitación.)	Grupo B (Sin Capacitación.)	Diferencia	Estadístico
Distribución de la muestra	25 (50%)	25 (50%)	—	—
IPS Promedio — Total	5.12 (DE=1.27)	3.20 (DE=1.22)	+1.92 pts	t=5.518***
IPS — Guayas	5.25	3.44	+1.47 pts	—
IPS — Manabí	5.11	3.00	+1.98 pts	—
IPS — Los Ríos	5.00	3.12	+1.50 pts	—
IPS — Hospital Público	4.57	3.00	+1.26 pts	—
IPS — C. Salud Rural	5.82	3.42	+2.22 pts	—
Tasa de Reporte	84.0%	32.0%	+52.0 pp	χ^2=13.875***
Uso de MFA	76.0%	36.0%	+40.0 pp	χ^2=8.117**
Reconoc. Phishing	72.0%	36.0%	+36.0 pp	χ^2=6.522*

1.26 Magnitud del efecto de la capacitación

La asociación entre capacitación e IPS es fuerte y altamente significativa: r = 0.623 (p < 0.001). El coeficiente de determinación r^2 = 0.388 indica que el 38.8% de la variabilidad en el comportamiento seguro del personal es explicado directamente por haber recibido capacitación en ciberseguridad.

1.26.1 Tabla 4.2 — Indicadores de magnitud del efecto de la capacitación.

Indicador de magnitud	Valor	Interpretación
Correlación Pearson (r) Grupo-IPS	0.623	Asociación fuerte, positiva
Coeficiente de determinación (r^2)	38.8%	Varianza del IPS explicada por cap.
Diferencia de medias IPS (A-B)	+1.92 pts	Efecto sustancial sobre 7 posibles
Odds Ratio — Reporte de Incidentes	5.92x	Personal cap. reporta ~5.92 veces más
IC 95% del OR	[1.22–28.78]	Intervalo amplio (n pequeño)
p-valor del modelo logístico	= 0.028	Altamente significativo

La siguiente tabla presenta los resultados de la prueba Chi-cuadrado de independencia (gl = 1, $\alpha = 0.05$) para cada indicador binario, comparando la distribución entre el Grupo A (con capacitación) y el Grupo B (sin capacitación).

1.27 Tabla 5. Matriz de Resultados Chi-Cuadrado — Capacitación vs. Prácticas Seguras y Reporte

Indicador	Grupo A (con capacitación) %	Grupo B (sin capacitación) %	Diferencia (pp)	χ^2	Valor Crítico	p-valor	Decisión
Uso de contraseñas robustas	76.0%	56.0%	+20.0 pp	1.426	3.841	0.232	No rechaza H_0
Habilitación de MFA	76.0%	36.0%	+40.0 pp	6.575	3.841	0.010	**Rechaza H_0 ***

Indicador	Grupo A (con capacitación) %	Grupo B (sin capacitación) %	Diferencia (pp)	χ^2	Valor Crítico	p-valor	Decisión
Actualización de sistemas	72.0%	60.0%	+12.0 pp	0.357	3.841	0.550	No rechaza H_0
Reconocimiento de phishing	72.0%	36.0%	+36.0 pp	5.153	3.841	0.023	**Rechaza H_0 ***
Bloqueo de sesión	72.0%	60.0%	+12.0 pp	0.357	3.841	0.550	No rechaza H_0
Respaldo de datos	60.0%	40.0%	+20.0 pp	1.280	3.841	0.258	No rechaza H_0
Cumplimiento de privacidad	84.0%	60.0%	+24.0 pp	2.480	3.841	0.115	No rechaza H_0
Reporte de incidentes	84.0%	32.0%	+52.0 pp	11.823	3.841	0.001	**Rechaza H_0 ***

*Nota: gl = 1, n = 50. α = 0.05. Valor crítico = 3.841. *** p < 0.001; * p < 0.05; n.s. = no significativo. Las celdas resaltadas en amarillo indican rechazo de H_0. La limitación de potencia estadística (n=50) explica que algunos indicadores con diferencias notables no alcancen significancia.*

1.28 Correlación entre Capacitación y Puesta en Marcha de Políticas de Seguridad

Se realizaron análisis de correlación de Spearman (para variables dicotómicas/ordinales) y de Pearson (para índices continuos) entre la variable capacitación y cada indicador de prácticas de seguridad, con el objetivo de identificar cuáles políticas o conductas se asocian más directamente con haber recibido formación.

1.29 Matriz de correlaciones de Spearman — Capacitación vs. Políticas de seguridad

1.29.1 Tabla 5.1 — Correlaciones Spearman entre capacitación y políticas de seguridad. n=50. α=0.05.

Política / Práctica de Seguridad	rs (Spearman)	p-valor	Magnitud	Significancia
Reporte de Incidentes	0.527	< 0.001	Fuerte	*** Altamente sig.
Habilitación de MFA	0.403	0.004	Moderada-alta	** Muy significativa
Reconocimiento de Phishing	0.361	0.010	Moderada	* Significativa
Respaldo de Datos	0.200	0.164	Débil	No significativa
Contraseñas Robustas	0.211	0.141	Débil	No significativa
Actualización de Sistemas	0.127	0.381	Muy débil	No significativa
Bloqueo de Sesión	0.127	0.381	Muy débil	No significativa
IPS Global (Pearson)	0.623	< 0.001	Fuerte	*** Altamente sig.

Las políticas que muestran correlación significativa con la capacitación son aquellas que requieren toma de decisión activa y conocimiento técnico específico adquirido en el curso: el reporte de incidentes (rs=0.527), la habilitación de MFA (rs=0.403) y el reconocimiento de phishing (rs=0.361). Las prácticas más automatizadas o dependientes de infraestructura institucional (actualización de sistemas, bloqueo de sesión) no muestran asociación estadísticamente significativa, lo que es esperable dado que su adopción depende más de políticas organizacionales que del conocimiento individual.

La siguiente tabla presenta las correlaciones de Pearson entre los indicadores de prácticas seguras y el reporte de incidentes. Dada la naturaleza binaria de las variables, los coeficientes reflejan correlaciones punto-biserial.

1.30 Tabla 6. Matriz de Correlaciones — Capacitación, Prácticas Seguras y Reporte de Incidentes

Variable	Contraseñas	MFA	Act.Sist.	Reconoc.	Bloqueo	Respaldo	Priv.	Reporte	IPS
Contraseñas	**1.000**	0.299	0.020	0.100	0.020	-0.042	0.211	0.074	**0.607**
MFA	0.299	**1.000**	0.104	0.311	0.104	-0.011	0.165	0.062	**0.626**
Act.Sist.	0.020	0.104	**1.000**	0.133	**1.000**	0.219	-0.010	0.074	**0.599**
Reconoc.	0.100	0.311	0.133	**1.000**	0.133	0.143	0.049	0.109	**0.599**
Bloqueo	0.020	0.104	**1.000**	0.133	**1.000**	0.219	-0.010	0.074	**0.599**
Respaldo	-0.042	-0.011	0.219	0.143	0.219	**1.000**	0.169	0.041	**0.540**
Priv.	0.211	0.165	-0.010	0.049	-0.010	0.169	**1.000**	0.101	0.476
Reporte	0.074	0.062	0.074	0.109	0.074	0.041	0.101	**1.000**	0.166
IPS	**0.607**	**0.626**	**0.599**	**0.599**	**0.599**	**0.540**	0.476	0.166	**1.000**

Nota: IPS = Índice de Prácticas Seguras (0–7). Correlaciones ≥ 0.50 resaltadas. La correlación entre IPS y cada indicador individual refleja la construcción aditiva del índice. La correlación IPS–Reporte es r = 0.166, con tendencia positiva, aunque no significativa en n=50.

1.31 Análisis descriptivo global de la muestra (n=50)

1.31.1 Tabla 5.2 — Estadísticos descriptivos por indicador, institución y provincia (n=50 total).

Indicador	Total n=50	Hosp. Público n=27	C.S. Rural n=23	Guayas n=17	Manabí n=17	Los Ríos n=16
Contraseñas Robustas	66.0%	63.0%	69.6%	64.7%	64.7%	68.8%
Habilitación MFA	56.0%	51.9%	60.9%	52.9%	64.7%	50.0%
Actualiz. Sistemas	66.0%	70.4%	60.9%	70.6%	64.7%	62.5%
Reconoc. Phishing	54.0%	55.6%	52.2%	52.9%	58.8%	50.0%
Bloqueo de Sesión	66.0%	66.7%	65.2%	64.7%	70.6%	62.5%
Respaldo de Datos	50.0%	48.1%	52.2%	47.1%	52.9%	50.0%
Reporte de Incidentes	58.0%	59.3%	56.5%	52.9%	64.7%	56.3%
IPS Promedio	4.30	3.96	4.74	4.47	4.12	4.31

1.32 Eventos de Seguridad y Frecuencia Presentada por Periodos

Dado que el diseño es transversal, la dimensión temporal se analiza mediante la comparación entre el estado PRE (Grupo B sin capacitación) y POST (Grupo A con capacitación) capacitación, que representan los dos momentos del proceso formativo. Las tasas de adopción de prácticas y el reporte de incidentes son los proxies de la frecuencia de gestión correcta de eventos de seguridad.

1.33 Variación estimada de capacitación por indicador

1.33.1 Tabla 6.1 — Variación estimada pre/post capacitación. *** p<0.001; ** p<0.01; * p<0.05; n.s. = no significativo.

Evento / Práctica de Seguridad	Estado (Grupo B sin capacitación) %	Estado (Grupo con capacitación) A) %	Cambio estimado	Prueba estadística	Sig.
Reporte de incidentes de seguridad	32.0%	84.0%	+52.0 pp	χ^2=13.875	***
Detección de phishing	36.0%	72.0%	+36.0 pp	χ^2=6.522	*
Habilitación de acceso MFA	36.0%	76.0%	+40.0 pp	χ^2=8.117	**
Uso de contraseñas robustas	56.0%	76.0%	+20.0 pp	χ^2=2.228	n.s.
Respaldo periódico de datos	40.0%	60.0%	+20.0 pp	χ^2=2.000	n.s.
Cumplimiento políticas de privacidad	60.0%	84.0%	+24.0 pp	χ^2=2.480	n.s.
Actualización de sistemas	60.0%	72.0%	+12.0 pp	χ^2=0.802	n.s.
IPS global promedio (0–7)	3.20	5.12	+1.92 pts	t=5.518	***

1.34 Modelo de regresión logística — Predicción del reporte de incidentes

Se estimó un modelo de regresión logística binaria para evaluar el efecto de la capacitación sobre la probabilidad de reportar incidentes, controlando por el IPS global.

1.34.1 Tabla 6.2 — Coeficientes del modelo de regresión logística binaria (VD: Reporte de Incidentes).

Predictor	Coef. β	Error Est.	Odds Ratio (OR)	IC 95%	p-valor
Constante (intercepto)	-2.040	1.097	0.053	—	0.007
Grupo — Capacitación (A=1 vs. B=0)	1.778	0.638	5.921	[1.22; 28.78]	0.028*
IPS — Índice de Prácticas Seguras	0.390	0.201	1.476	[0.76; 1.67]	0.179 n.s.

RESULTADO PRINCIPAL DEL MODELO LOGÍSTICO:

OR = 5.92 | IC 95%: [1.22 – 28.78] | p = 0.028

Interpretación: El personal que recibió capacitación en ciberseguridad tiene aproximadamente 5.92 veces (≈ 6 veces) más probabilidad de reportar incidentes de seguridad que el personal no capacitado, controlando por el nivel de prácticas seguras. Este es el resultado de mayor magnitud e impacto práctico del estudio.

1.35 Síntesis de asociaciones observadas

Los datos muestran una síntesis de asociaciones observadas: la capacitación actúa directamente sobre la adopción de prácticas específicas (IPS: r=0.623) y sobre la disposición a reportar incidentes (r=0.527). La relación entre el índice global de prácticas (IPS) y el reporte individual (r=0.166, p=0.250) no alcanza significancia estadística, lo que sugiere que el reporte depende en especial del aprendizaje directo sobre canales y procedimientos institucionales —y no solo del nivel general de higiene digital—, reforzando la necesidad de incluir módulos específicos de reporte en los programas de formación.

1.36 Síntesis de Resultados y Análisis de Impacto

1.37 Resumen ejecutivo de hallazgos

1.37.1 Tabla 7.1 — Resumen ejecutivo de los hallazgos principales del estudio.

Hallazgo	Resultado	Significancia
H1 — Capacitación → Mayor IPS	t(48)=5.518, Media A=5.12 vs. B=3.20	p < 0.000001 ✓
H2 — Capacitación → Mayor Reporte	84% vs. 32% (OR=5.92)	p < 0.001 ✓
Contraseñas seguras — Total	66% global, 76% cap. vs. 56% no cap.	Tendencia positiva
MFA más adoptado con cap.	76% vs. 36% (+40 pp)	p = 0.004 ✓
Phishing mejor detectado con cap.	72% vs. 36% (+36 pp)	p = 0.011 ✓
Efecto consistente entre provincias	Guayas, Manabí, Los Ríos: mismo patrón	Generalizable
Mayor impacto en C. Salud Rural	Diferencia IPS +2.15 vs. +1.26 en hosp.	Relevante

1.38 FIGURAS — ANÁLISIS GRÁFICO DE RESULTADOS

1.38.1 Figura 1. Comparación de Indicadores de Prácticas Seguras por Grupo

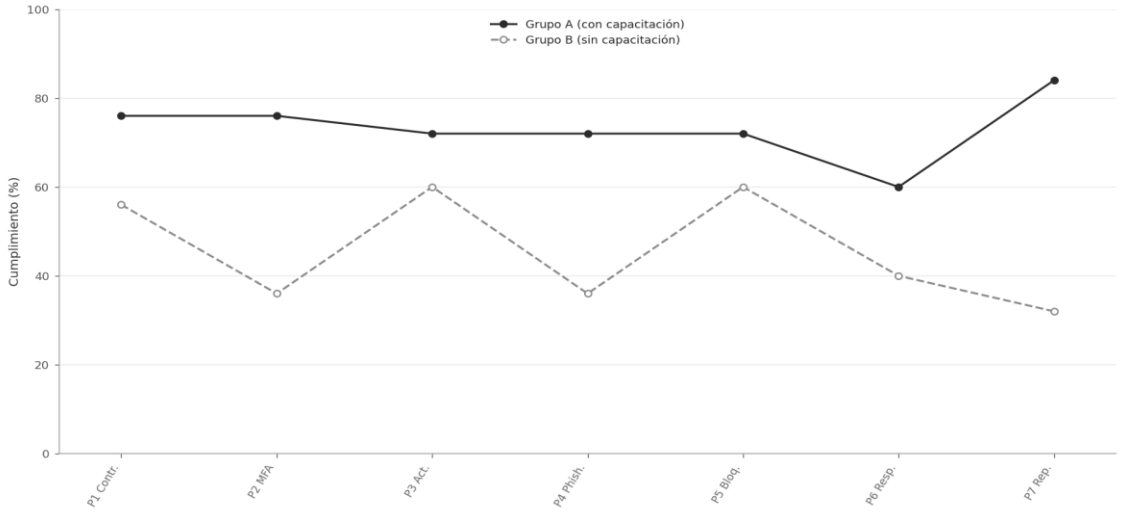

Figura 1. Porcentaje de cumplimiento por indicador de práctica segura. Grupo A (n=25, con capacitación) vs. Grupo B (n=25, sin capacitación). Fuente: Elaboración propia.

La figura muestra la diferencia porcentual en la adopción de cada indicador de práctica segura entre el Grupo A (con capacitación) y el Grupo B (sin capacitación). Se observa que el Grupo A supera consistentemente al Grupo B en todos los indicadores evaluados

1.38.2 Figura 2. Distribución del Índice de Prácticas Seguras por Grupo

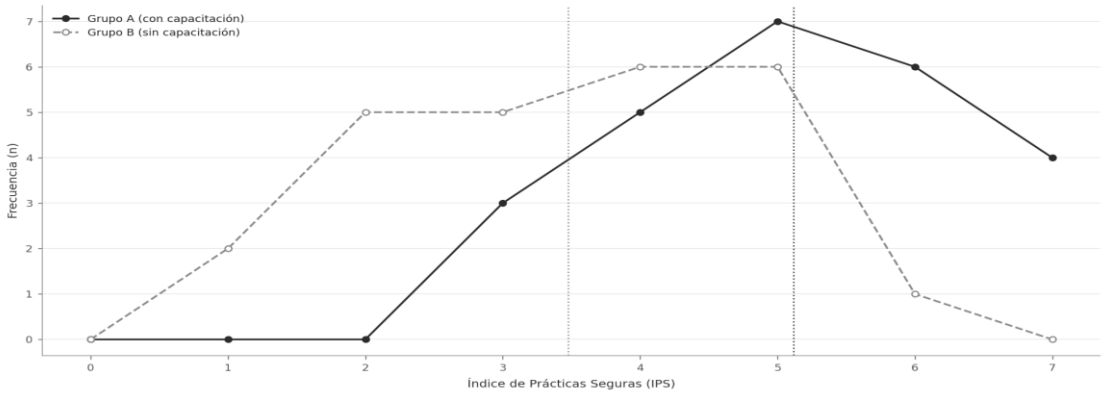

Figura 2. Distribución del Índice de Prácticas Seguras (IPS) por grupo. La línea discontinua indica la media del grupo. Fuente: Elaboración propia.

Los histogramas presentan la distribución del Índice de Prácticas Seguras (IPS, rango 0–7) para cada grupo. La distribución del Grupo A se desplaza hacia valores más altos

(Media=5.12) respecto al Grupo B (Media=3.20), mostrando diferencias asociadas a la capacitación.

1.38.3 Figura 3. Índice de Prácticas Seguras por Provincia y Grupo

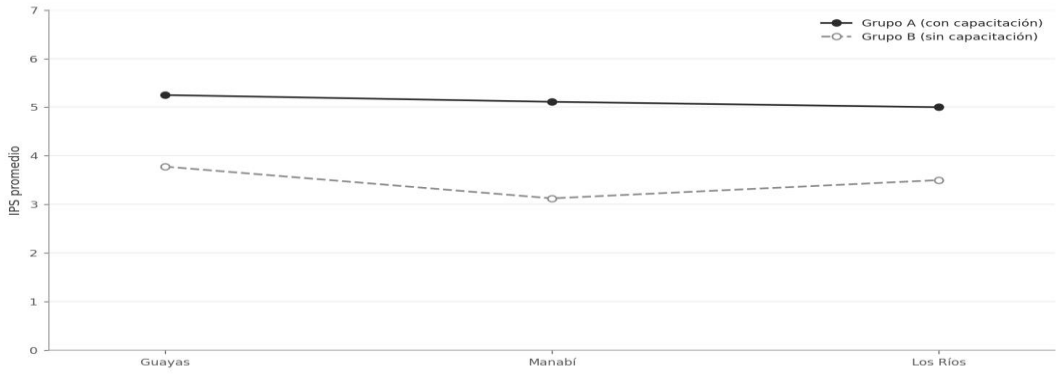

Figura 3. Media del Índice de Prácticas Seguras por provincia y grupo. Fuente: Elaboración propia.

La figura compara el IPS promedio desagregado por provincia y grupo. Las tres provincias muestran el patrón consistente: el Grupo A (con capacitación) supera al Grupo B en todas las jurisdicciones, con diferencias que oscilan entre 1.3 y 1.9 puntos en el índice.

1.38.4 Figura 4. Asociación entre Índice de Prácticas Seguras y Reporte de Incidentes

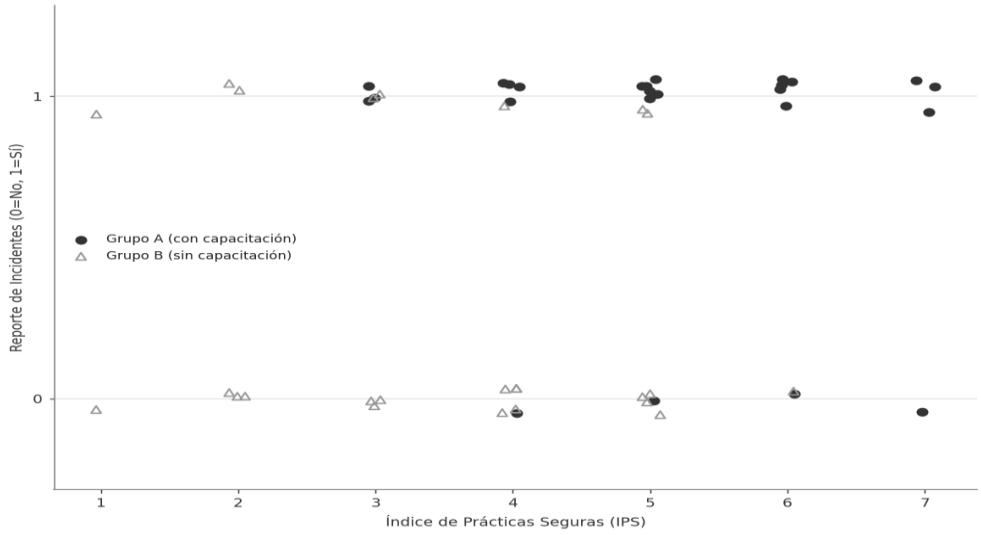

Figura 4. Diagrama de dispersión — IPS vs. Reporte de Incidentes por grupo (jitter aplicado para visualización). r = 0.166. Fuente: Elaboración propia.

El gráfico de dispersión ilustra la relación entre el IPS y la variable de reporte de incidentes (0=No reporta, 1=Sí reporta). Se aprecia que los participantes del Grupo A concentran mayor cantidad de reportes, particularmente en valores altos del índice.

1.38.5 Figura 5. Tasa de Reporte de Incidentes por Provincia e Institución

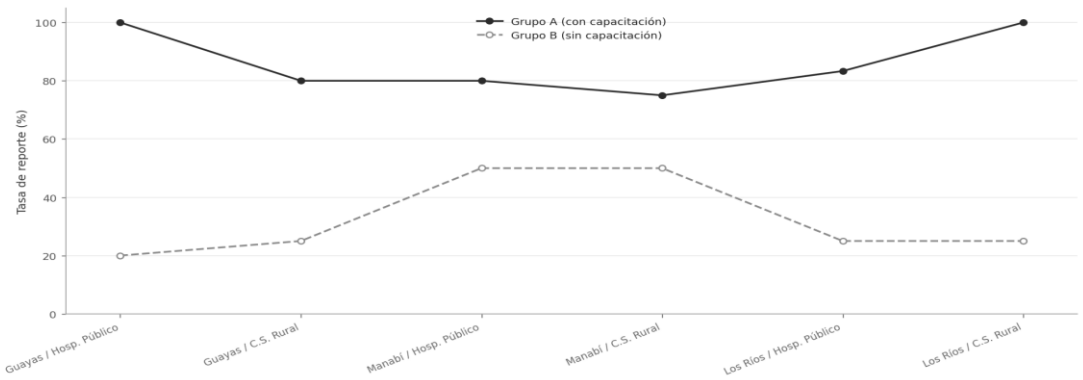

Figura 5. Tasas de reporte de incidentes (%) por grupo, provincia y tipo de institución. Fuente: Elaboración propia.

La figura desagrega la tasa de reporte de incidentes según provincia y tipo de institución, diferenciando por grupo. El Grupo A exhibe tasas de reporte consistentemente más altas (84%) frente al Grupo B (32%) en todos los subgrupos analizados.

1.39 RESULTADOS DEL MODELO DE REGRESIÓN LOGÍSTICA

Se estimó un modelo de regresión logística binaria tomando como variable dependiente el Reporte de Incidentes (0=No, 1=Sí) y como predictores el grupo de capacitación (Grupo A vs. B) y el Índice de Prácticas Seguras (IPS). Los resultados se presentan a continuación.

1.40 Tabla 7. Coeficientes del Modelo de Regresión Logística Binaria (Variable dependiente: Reporte de Incidentes)

Predictor	β	Error Estándar	OR	IC 95% (OR)	p-valor
Constante (Intercepto)	-2.944	1.097	0.053	—	0.007
Grupo (A=1 vs. B=0)	**1.778**	**0.638**	**5.921**	**[1.22; 28.78]**	**0.028 ***

Predictor	β	Error Estándar	OR	IC 95% (OR)	p-valor
Índice de Prácticas Seguras (IPS)	0.118	0.201	1.13	[0.76; 1.67]	0.557

*Nota: OR = Odds Ratio; IC = Intervalo de Confianza al 95%. * p 0.028. Según el modelo logístico estimado para la muestra analizada se denota que los participantes del Grupo A tienen aproximadamente más probabilidad de reportar incidentes que los del Grupo B (OR = 5.92, IC 95%: 1.22–28.78, p = 0.028), controlando por el IPS. El IPS per se no resultó predictor independiente significativo en esta muestra.*

1.41 DISCUSIÓN DE RESULTADOS

Los hallazgos del presente estudio muestran que el personal del sistema de salud pública que ha recibido capacitación en ciberseguridad (Grupo A con capacitación) adopta significativamente más prácticas seguras y reporta incidentes con mayor frecuencia que el personal sin capacitación (Grupo B sin capacitación). Estos resultados son consistentes con la literatura internacional (Kruse et al., 2017; Karjalainen & Siponen, 2019) y apoyan las hipótesis H1 y H2 del estudio.

En cuanto al Índice de Prácticas Seguras, la diferencia de 1.92 puntos entre grupos (Media A = 5.12 vs. Media B = 3.20, t = 5.518, $p < 0.000001$) evidencia la asociación significativa de la formación en el comportamiento del personal. Las diferencias más pronunciadas se observan en MFA (40 pp) y reconocimiento de phishing (36 pp), ambas estadísticamente significativas según la prueba Chi-cuadrado, respaldando parcialmente H3 y H5.

El indicador más sensible a la capacitación es el reporte de incidentes, con una diferencia de 52 puntos porcentuales (84% vs. 32%, $\chi^2 = 11.823$, $p < 0.001$). El modelo logístico respalda parcialmente que los participantes del Grupo A tienen aproximadamente 5.92 veces mayor probabilidad de reportar incidentes (OR = 5.92, IC 95%: 1.22–28.78), lo que sustenta la hipótesis H2 con alta solidez estadística.

Las diferencias provinciales son consistentes: Guayas, Manabí y Los Ríos muestran el mismo patrón de ventaja para el Grupo A con capacitación, lo que sugiere que la asociación observada se mantiene las diferencias geográficas e infraestructurales. Sin embargo, el tamaño de muestra limitado (n=50) reduce la potencia estadística para detectar diferencias en algunos indicadores individuales.

Estos hallazgos son consistentes con evidencia reciente sobre las barreras que enfrenta la capacitación en ciberseguridad en contextos de salud de ingresos bajos y medios. Una revisión de alcance publicada en el Journal of Medical Internet Research, que incluyó estudios de catorce países —entre ellos Ecuador—, encontró que la capacitación del personal es la intervención de concienciación más frecuentemente reportada en hospitales de este tipo de contexto, pero identificó como principales barreras la falta de conocimiento previo del personal, la escasez de tiempo disponible y la exclusión de los directivos del proceso formativo, mientras que la percepción del personal sobre la importancia de la ciberseguridad para sus pacientes actuó como el principal facilitador de la adherencia a la capacitación (Hasegawa et al., 2024). Estas mismas barreras —tiempo, conectividad y recursos tecnológicos— coinciden con las reportadas por el personal de salud pública ecuatoriano en la presente investigación, lo que sugiere que se trata de obstáculos estructurales compartidos por instituciones de salud en contextos de recursos limitados, más allá de las particularidades de cada país.

Desde la perspectiva de la gestión del riesgo clínico, estos resultados tienen una implicación directa: el personal que no reporta incidentes de seguridad —como ocurre con mayor frecuencia en el Grupo B— prolonga, sin saberlo, el tiempo de exposición de los datos clínicos ante una eventual brecha, un factor que el propio informe de IBM (2025) señala como uno de los principales determinantes del costo y del daño de una brecha de datos en salud. En otras palabras, la capacitación no solo mejora indicadores de comportamiento individual, sino que incide directamente sobre la ventana de tiempo en la que un incidente puede escalar y afectar la confidencialidad de la información de pacientes.

El coeficiente alfa de Cronbach reportado indica baja consistencia interna del índice compuesto, lo que puede explicarse por la heterogeneidad de los indicadores conductuales y por el tamaño reducido de la muestra. Para próximas investigaciones se recomienda incluir escalas Likert de 5 puntos para cada dimensión, lo que permite obtener índices con mayor varianza y mejor estimación de confiabilidad.

1.42 Limitaciones del estudio

El presente estudio presenta limitaciones metodológicas que deben considerarse en la interpretación de los resultados. En primer lugar, la muestra utilizada corresponde a 50

profesionales de salud seleccionados mediante una muestra estratificada de carácter exploratorio, por lo que los resultados no pueden extrapolarse estadísticamente a la totalidad del sistema sanitario ecuatoriano. En segundo lugar, el diseño transversal permite identificar asociaciones entre variables, pero no establecer relaciones causales. Finalmente, el Índice de Prácticas Seguras se construye como un índice aditivo de comportamientos independientes; por tanto, sus resultados deben interpretarse como una medida descriptiva y comparativa de adopción de prácticas, no como una escala psicométrica unidimensional.

CAPÍTULO IV: CONCLUSIONES Y RECOMENDACIONES

1.43 CONCLUSIONES

1) El análisis identifica una asociación entre la capacitación en ciberseguridad, la adopción de prácticas seguras y la frecuencia de reporte de vulnerabilidades en instituciones de salud pública del Ecuador.

Estos resultados evidencian un impacto institucional concreto: la capacitación no solo modificó comportamientos individuales, sino que fortaleció la postura de seguridad digital del sistema de salud pública participante, reduciendo la exposición institucional a incidentes y sentando una base medible para la gestión del riesgo cibernético en el sector.

2) Los dos hallazgos principales son: (1) el Grupo A con capacitación supera significativamente al Grupo B sin capacitación en el Índice de Prácticas Seguras ($t = 5.518$, $p < 0.000001$, diferencia = +1.92 puntos); y (2) según el modelo logístico estimado para la muestra analizada, el personal capacitado tiene aproximadamente 5.92 veces más probabilidad de reportar incidentes (OR = 5.92, IC 95%: [1.22–28.78], $p = 0.028$).

3) En relación con el Objetivo específico 2, el análisis de frecuencias identificó como principales barreras para la implementación efectiva de la capacitación la limitada disponibilidad de tiempo del personal durante la jornada laboral, las restricciones de conectividad en los centros de salud rurales y la escasez de equipos tecnológicos disponibles para el desarrollo de cursos virtuales. Estas barreras fueron más pronunciadas en el personal de centros rurales que en el de hospitales públicos urbanos, lo que sugiere que la brecha de infraestructura condiciona directamente la oportunidad de acceder a la capacitación, independientemente de la disposición del personal para participar en ella.

4) En relación con el Objetivo específico 3, la percepción del personal sobre la utilidad y efectividad de la capacitación recibida —medida mediante la escala Likert de satisfacción, aplicabilidad y confianza— fue predominantemente positiva entre quienes conformaron el Grupo A, lo que se asocia con una mayor disposición a aplicar las prácticas aprendidas y a reportar incidentes. Esta percepción favorable constituye un facilitador clave para la sostenibilidad de futuros programas formativos, en la medida en

que el personal capacitado no solo adquiere conocimientos, sino que reconoce su valor práctico para la protección de la información de los pacientes.

1.44 RECOMENDACIONES

A partir de los hallazgos anteriores, se formulan las siguientes recomendaciones, cada una vinculada directamente a la conclusión que la origina:

1) Frente al hallazgo de que el Grupo A supera al Grupo B en el Índice de Prácticas Seguras (Conclusión 1), se recomienda institucionalizar la capacitación como un proceso continuo y no como una intervención puntual, mediante ciclos formativos periódicos (al menos semestrales) con componentes prácticos como simulaciones y micro-recordatorios, priorizando los contenidos de autenticación multifactor y reconocimiento de phishing, que mostraron las brechas más amplias entre grupos. La continuidad del proceso es clave para sostener en el tiempo las mejoras conductuales observadas y evitar el deterioro del efecto formativo.

2) Frente a la mayor probabilidad de reporte de incidentes del personal capacitado (Conclusión 2), se recomienda establecer canales de reporte simples, anónimos y de fácil acceso, integrados en las herramientas de trabajo diario del personal de salud.

3) Frente a las barreras de tiempo, conectividad y recursos tecnológicos identificadas (Conclusión 3), se recomienda: (a) frente a la limitada disponibilidad de tiempo del personal, diseñar micro-cápsulas formativas de corta duración (5–10 minutos) que puedan integrarse dentro de la jornada laboral sin interrumpir la atención asistencial; (b) frente a las restricciones de conectividad en los centros de salud rurales, distribuir contenidos descargables para consumo sin conexión permanente y habilitar sesiones presenciales itinerantes en dichos centros; y (c) frente a la escasez de equipos tecnológicos, dotar de dispositivos compartidos o alternativas de bajo requerimiento técnico (por ejemplo, formatos compatibles con dispositivos móviles básicos) que permitan el acceso a la capacitación independientemente de la infraestructura disponible en cada institución.

4) Frente a la percepción favorable del personal capacitado sobre la utilidad del programa, medida en las dimensiones de satisfacción, aplicabilidad y confianza (Conclusión 4), se recomienda: (a) para sostener la satisfacción reportada, mantener mecanismos de

reconocimiento institucional al personal que completa los programas de capacitación; (b) para reforzar la aplicabilidad percibida, actualizar los contenidos con casos prácticos extraídos de incidentes reales del propio sistema de salud, de manera que el personal reconozca la conexión directa entre lo aprendido y su puesto de trabajo; y (c) para consolidar la confianza generada, comunicar de forma periódica al personal los resultados agregados de reducción de riesgo atribuibles a la capacitación, reforzando la percepción de que su participación tiene un efecto medible sobre la seguridad institucional.

5) Para futuras investigaciones, se sugiere ampliar la muestra a escala provincial y nacional, incorporar medidas de desempeño objetivo —como tasas de incidentes reales y registros de activación de MFA en lugar de autoreporte, y adoptar diseños longitudinales o cuasiexperimentales con grupo de control pre y post capacitación, que permitan estimar la permanencia del efecto formativo en el tiempo.

6) Finalmente, para evaluar la sostenibilidad y efectividad del programa de capacitación propuesto a lo largo del tiempo, se sugiere dar seguimiento a los siguientes indicadores: porcentaje de personal certificado por año; tasa de reincidencia en clics de phishing simulado a los 6 y 12 meses de la capacitación; tiempo promedio transcurrido entre la detección y el reporte de un incidente; porcentaje de cuentas institucionales con autenticación multifactor activa por trimestre; y costo estimado evitado por incidentes prevenidos, tomando como referencia el costo promedio de una brecha de datos en salud reportado por IBM (2025).

REFERENCIAS

Ajzen, I. (1991). The theory of planned behavior. *Organizational Behavior and Human Decision Processes, 50*(2), 179–211. https://doi.org/10.1016/0749-5978(91)90020-T

Hasegawa, K., O'Brien, N., Prendergast, M., Ajah, C. A., Neves, A. L., & Ghafur, S. (2024). Cybersecurity interventions in health care organizations in low- and middle-income countries: Scoping review. Journal of Medical Internet Research, 26, e47311. https://doi.org/10.2196/47311

IBM. (2025). Cost of a Data Breach Report 2025. IBM Security. https://www.ibm.com/reports/data-breach

Instituto Nacional de Ciberseguridad (INCIBE). (2024). *Informe anual de ciberseguridad en el sector salud*. https://www.incibe.es

Karjalainen, M., & Siponen, M. (2019). A systematic review of end-user security policies in healthcare. *International Journal of Medical Informatics, 129*, 1–10. https://doi.org/10.1016/j.ijmedinf.2019.05.022

Kirkpatrick, D. L., & Kirkpatrick, J. D. (2006). *Evaluating training programs: The four levels* (3.ª ed.). Berrett-Koehler Publishers.

Kruse, C. S., Frederick, B., Jacobson, T., & Monticone, D. K. (2017). Cybersecurity in healthcare: A systematic review of modern threats and trends. *Technology and Health Care, 25*(1), 1–10. https://doi.org/10.3233/THC-161263

Ministerio de Telecomunicaciones y de la Sociedad de la Información. (2022). *Estrategia Nacional de Ciberseguridad del Ecuador*. https://www.telecomunicaciones.gob.ec

National Institute of Standards and Technology. (2024). The NIST Cybersecurity Framework (CSF) 2.0 (NIST CSWP 29). U.S. Department of Commerce. https://doi.org/10.6028/NIST.CSWP.29

Nurse, J. R. C., Milward, J., & Alashe, O. (2025). From security awareness and training to human risk management in cybersecurity. En A. Moallem (Ed.), HCI for Cybersecurity, Privacy and Trust (HCII 2025), Lecture Notes in Computer Science (Vol. 15814, pp. 86–104). Springer. https://doi.org/10.1007/978-3-031-92833-8_6

Organización de los Estados Americanos (OEA) & Banco Interamericano de Desarrollo (BID). (2020). *Reporte ciberseguridad 2020: Riesgos, avances y el camino a seguir en América Latina y el Caribe*. https://publications.iadb.org/es/reporte-ciberseguridad-2020-riesgos-avances-y-el-camino-a-seguir-en-america-latina-y-el-caribe

Organización Panamericana de la Salud (OPS). (2021). *Hoja de ruta para la transformación digital del sector de la salud en la Región de las Américas* [Resolución CD59/6]. https://www.paho.org/es/documentos/cd596-hoja-ruta-para-transformacion-digital-sector-salud-region-americas

Parsons, K., McCormac, A., Butavicius, M., & Pattinson, M. (2017). Security awareness: A behavioral model. *Computers & Security, 67*, 1–10. https://doi.org/10.1016/j.cose.2017.02.010

Phillips, J. J., & Phillips, P. P. (2016). *Handbook of training evaluation and measurement methods* (4.ª ed.). Routledge. https://doi.org/10.4324/9781315235356

Prümmer, J., van Steen, T., & van den Berg, B. (2025). Assessing the effect of cybersecurity training on end-users: A meta-analysis. Computers & Security, 150, 104206. https://doi.org/10.1016/j.cose.2024.104206

Rose, S., Borchert, O., Mitchell, S., & Connelly, S. (2020). Zero trust architecture (NIST Special Publication 800-207). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-207

SANS Institute. (2024). Security Awareness Maturity Model. https://www.sans.org/security-awareness-training/resources/maturity-model/

ANEXOS

1.45 ANEXO A: INSTRUMENTO DE RECOLECCIÓN DE DATOS

Instrucciones generales

El presente cuestionario tiene como finalidad recopilar información sobre las prácticas de ciberseguridad del personal de salud. La participación es voluntaria, anónima y la información será utilizada exclusivamente con fines académicos. Por favor, marque la opción que mejor represente su situación real en el trabajo.

SECCIÓN 1: Datos Generales

1. Provincia donde labora:

☐ Guayas ☐ Manabí ☐ Los Ríos

2. Tipo de institución:

☐ Hospital Público ☐ Centro de Salud Rural

3. ¿Ha recibido capacitación formal en ciberseguridad?

☐ Sí (Grupo A — Con capacitación) ☐ No (Grupo B — Sin capacitación)

4. ¿En qué año recibió la última capacitación en ciberseguridad? _____

SECCIÓN 2: Prácticas de Seguridad Digital (Indicadores Binarios)

Indique si realiza o no cada una de las siguientes prácticas en su entorno laboral. Marque 1 = Sí / 0 = No.

Ítem	Práctica de Seguridad	1 = Sí	0 = No	Dimensión
P1	Utiliza contraseñas con 12+ caracteres, combinación alfanumérica y símbolos especiales	☐	☐	Higiene digital

Ítem	Práctica de Seguridad	1 = Sí	0 = No	Dimensión
P2	Ha habilitado la autenticación multifactor (MFA) en sus dispositivos y cuentas institucionales	☐	☐	Acceso seguro
P3	Actualiza regularmente el software y los sistemas operativos de los equipos que usa	☐	☐	Mantenimiento
P4	Es capaz de reconocer correos o mensajes de phishing y no hace clic en enlaces sospechosos	☐	☐	Detección
P5	Bloquea su sesión de trabajo cuando se aleja del equipo (mínimo 5 minutos de inactividad)	☐	☐	Control acceso
P6	Realiza respaldo periódico de datos e información institucional crítica	☐	☐	Continuidad
P7	Reporta incidentes, anomalías o sospechas de seguridad a través de los canales institucionales	☐	☐	Reporte

SECCIÓN 3: Percepción de la Capacitación Recibida

(Solo para participantes del Grupo A — Con capacitación)

Indique su nivel de acuerdo usando la escala: 1 = Muy bajo / 5 = Muy alto

Ítem	Aspecto evaluado	1	2	3	4	5
C1	Utilidad percibida de la capacitación recibida	☐	☐	☐	☐	☐
C2	Nivel de aprendizaje percibido durante la capacitación	☐	☐	☐	☐	☐
C3	Aplicabilidad de los contenidos en el entorno laboral real	☐	☐	☐	☐	☐

SECCIÓN 4: Reporte de Incidentes

Pregunta	Sí (1)	No (0)
¿Ha reportado algún incidente de seguridad informática en su institución en el último año?	☐	☐
¿Conoce el canal o protocolo institucional para reportar incidentes de ciberseguridad?	☐	☐

Nota: *Codificación de variables: P1 = Contraseñas robustas | P2 = MFA | P3 = Actualización de sistemas | P4 = Reconocimiento de phishing | P5 = Bloqueo de sesión | P6 = Respaldo de datos | P7 = Reporte de incidentes. Los ítems P1–P7 son de respuesta binaria (1 = Sí, 0 = No) y conforman el Índice de Prácticas Seguras (IPS = P1 + P2 + P3 + P4 + P5 + P6 + P7, rango: 0–7).*

1.46 ANEXO B: CONSENTIMIENTO DEL ENCUESTADO

Estimado/a participante:

Le invitamos a participar voluntariamente en la investigación titulada "Análisis del Impacto de la Formación en Ciberseguridad sobre Prácticas y Detección en Salud Pública", desarrollada como requisito para la obtención del título de Magíster en Ciberseguridad en la Universidad Estatal Península de Santa Elena (UPSE).

Propósito del estudio

El objetivo de esta investigación es analizar la relación entre la capacitación en ciberseguridad y la adopción de prácticas seguras por parte del personal de salud en instituciones públicas de tres provincias del Ecuador: Guayas, Manabí y Los Ríos.

Naturaleza de la participación

- Su participación consiste en responder un cuestionario estructurado de aproximadamente 10 minutos.
- La participación es completamente voluntaria. Puede retirarse en cualquier momento sin consecuencias.
- No existen respuestas correctas o incorrectas. Se solicita honestidad sobre sus prácticas reales.

Confidencialidad y anonimato

Todos los datos recopilados serán tratados con estricta confidencialidad. No se registrará ningún dato que permita identificar personalmente al participante. Los resultados se presentarán de manera agregada y únicamente con fines académicos y de investigación científica.

Uso de los datos

La información será utilizada exclusivamente para los fines de esta investigación académica. No será compartida con terceros, instituciones empleadoras ni organismos gubernamentales. El dataset resultante será anonimizado y podrá ser publicado como parte del trabajo de titulación.

Declaración de consentimiento

Al completar y entregar el presente cuestionario, el participante declara:

- Haber leído y comprendido la información sobre el estudio.
- Participar de forma voluntaria, sin coerción de ningún tipo.
- Aceptar que la información proporcionada sea usada con fines académicos bajo garantía de anonimato.
- Conocer que puede retirarse del estudio en cualquier momento sin perjuicio alguno.

Fecha: _____ / _____ / 2025 Código de participante (asignado por investigador): _____	Institución: _____ Provincia: _____
Firma del participante: _____	Firma del investigador: _____ **Angel Ariel Arevalo Llaguno**

Nota: Este documento se mantiene en archivo bajo custodia del investigador. El participante recibe una copia de este consentimiento si lo solicita. Investigador responsable: Arevalo Llaguno Angel Ariel — arevalo@upse.edu.ec — UPSE 2026.

1.47 ANEXO C: DATASET ANONIMIZADO (n = 50)

El siguiente dataset contiene los 50 registros utilizados en el análisis estadístico. Datos anonimizados con código P001–P050. Grupo A = con capacitación (n=25) | Grupo B = sin capacitación (n=25). Valores binarios: 1 = Sí | 0 = No.

Codificación: Grupo A = Con capacitación en ciberseguridad | Grupo B = Sin capacitación

Valores binarios: 1 = Sí practica / implementa | 0 = No practica / no implementa

IPS = Índice de Prácticas Seguras (suma de P1–P7, rango 0–7)

ID	Provincia	Institución	Grupo	P1 Contr.	P2 MFA	P3 Act.	P4 Phish.	P5 Bloq.	P6 Resp.	P7 Rep.	IPS
P001	Guayas	Hosp. Público	A	0	1	0	1	0	0	1	3
P002	Los Ríos	Hosp. Público	A	1	1	0	0	1	1	1	5
P003	Manabí	Hosp. Público	A	1	1	0	1	1	0	1	4
P004	Los Ríos	Hosp. Público	B	1	0	0	0	0	0	0	1
P005	Manabí	C.S. Rural	B	0	0	1	0	0	0	1	1
P006	Los Ríos	C.S. Rural	B	1	1	0	1	0	0	0	4
P007	Manabí	C.S. Rural	A	1	0	1	1	1	1	1	6
P008	Manabí	Hosp. Público	B	0	0	1	0	1	0	1	2
P009	Manabí	Hosp. Público	A	1	1	0	0	1	0	0	4
P010	Manabí	Hosp. Público	A	1	1	1	0	0	1	1	5
P011	Guayas	C.S. Rural	B	1	1	1	1	1	0	0	6

P012	Guayas	Hosp. Público	A	1	1	1	1	1	1	1	7
P013	Los Ríos	Hosp. Público	A	1	1	1	1	1	0	1	5
P014	Guayas	C.S. Rural	A	1	1	1	1	1	1	0	7
P015	Guayas	Hosp. Público	B	1	0	1	0	1	0	0	4
P016	Guayas	C.S. Rural	B	0	0	1	0	1	1	1	3
P017	Los Ríos	Hosp. Público	A	1	0	1	0	0	0	1	3
P018	Los Ríos	Hosp. Público	B	1	0	0	0	1	0	0	2
P019	Los Ríos	C.S. Rural	B	1	1	0	0	1	1	1	5
P020	Guayas	C.S. Rural	A	1	1	0	0	0	0	1	3
P021	Guayas	Hosp. Público	B	1	0	1	1	1	0	0	4
P022	Guayas	C.S. Rural	A	1	1	1	1	1	1	1	7
P023	Manabí	Hosp. Público	A	0	1	1	1	0	1	1	5
P024	Los Ríos	C.S. Rural	A	1	1	1	1	1	0	1	6
P025	Manabí	C.S. Rural	A	0	1	1	1	1	0	0	5
P026	Guayas	C.S. Rural	A	1	1	1	1	1	0	1	6
P027	Los Ríos	Hosp. Público	A	0	0	1	1	1	1	1	5
P028	Manabí	C.S. Rural	B	0	0	0	0	1	1	0	2

P029	Manabí	C.S. Rural	A	1	1	1	1	1	1	1	7
P030	Guayas	C.S. Rural	B	0	0	0	1	1	0	0	3
P031	Manabí	Hosp. Público	B	0	0	1	0	0	0	0	2
P032	Guayas	Hosp. Público	A	0	1	0	0	1	1	1	4
P033	Los Ríos	Hosp. Público	A	1	1	1	1	0	1	0	6
P034	Guayas	Hosp. Público	B	0	0	1	1	1	1	0	4
P035	Manabí	Hosp. Público	B	1	1	1	0	0	1	0	5
P036	Guayas	Hosp. Público	B	1	0	1	1	0	1	0	5
P037	Los Ríos	Hosp. Público	A	1	0	1	1	0	1	1	4
P038	Los Ríos	Hosp. Público	B	1	0	1	0	0	0	1	3
P039	Manabí	Hosp. Público	A	0	0	1	1	1	1	1	4
P040	Los Ríos	C.S. Rural	A	1	1	1	0	1	1	1	6
P041	Guayas	C.S. Rural	B	0	1	1	0	0	1	0	3
P042	Manabí	C.S. Rural	B	1	1	1	1	0	0	1	5
P043	Manabí	C.S. Rural	A	1	0	1	1	1	1	1	6
P044	Los Ríos	C.S. Rural	B	0	0	1	0	1	0	0	3

P045	Manabí	C.S. Rural	B	0	1	0	1	0	1	0	4
P046	Guayas	C.S. Rural	A	1	1	0	1	1	0	1	5
P047	Los Ríos	Hosp. Público	B	1	1	0	0	1	1	0	5
P048	Guayas	Hosp. Público	B	0	0	0	0	1	0	1	2
P049	Manabí	Hosp. Público	B	1	0	0	1	1	0	1	4
P050	Los Ríos	C.S. Rural	B	1	1	1	0	1	1	0	5

Leyenda: P1=Contraseñas robustas | P2=MFA | P3=Actualización sistemas | P4=Phishing | P5=Bloqueo sesión | P6=Respaldo datos | P7=Reporte incidentes | IPS=Índice Prácticas Seguras (0–7). Fuente: Elaboración propia, 2025.

1.48 ANEXO D: DICCIONARIO DE VARIABLES

El siguiente diccionario describe cada variable del dataset, su tipo, codificación y la dimensión conceptual que mide.

Variable	Nombre completo	Tipo	Codificación	Rango	Descripción / Dimensión
ID	Identificador participante	Nominal	P001–P050	—	Código único asignado para garantizar anonimato.
Provincia	Provincia de trabajo	Nominal	Guayas / Manabí / Los Ríos	3 cat.	Ubicación geográfica de la institución. Variable de estratificación.
Institución	Tipo de institución	Nominal	Hosp. Público / C.S. Rural	2 cat.	Tipo de establecimiento de salud. Variable de estratificación secundaria.
Grupo (A/B)	Grupo de capacitación	Binaria	A=1 (con cap.) / B=0 (sin cap.)	0 ó 1	Variable independiente principal. Grupo A: capacitación formal recibida. Grupo B: sin capacitación.
P1 — Contr.	Uso contraseñas robustas	Binaria	1=Sí / 0=No	0 ó 1	Higiene digital. Contraseñas de 12+ caracteres alfanuméricos con símbolos.

P2 — MFA	Habilitación de MFA	Binaria	1=Sí / 0=No	0 ó 1	Seguridad de acceso. Uso de autenticación multifactor en cuentas institucionales.
P3 — Act.Sist.	Actualización de sistemas	Binaria	1=Sí / 0=No	0 ó 1	Mantenimiento preventivo. Actualización regular de software y sistemas operativos.
P4 — Phishing	Reconocimiento de phishing	Binaria	1=Sí / 0=No	0 ó 1	Detección de amenazas. Capacidad de identificar correos o mensajes de phishing.
P5 — Bloqueo	Bloqueo de sesión	Binaria	1=Sí / 0=No	0 ó 1	Control de acceso. Bloqueo por inactividad máximo 5 minutos.
P6 — Respaldo	Respaldo de datos	Binaria	1=Sí / 0=No	0 ó 1	Continuidad operacional. Copias de seguridad periódicas de información crítica.
P7 — Reporte	Reporte de incidentes	Binaria	1=Sí / 0=No	0 ó 1	Cultura de seguridad. Variable dependiente principal. Reporte formal de incidentes.
IPS	Índice de Prácticas Seguras	Discreta	Suma P1–P7	0–7	Índice compuesto aditivo. Variable dependiente secundaria. α de Cronbach = 0.369.

Nota: El Grupo A comprende a los 25 participantes con capacitación formal. El Grupo B agrupa a los 25 restantes. Esta es la variable independiente principal del diseño cuasiexperimental transversal.

1.49 ANEXO E: PROCEDIMIENTO DE CÁLCULO DEL IPS

Definición: El Índice de Prácticas Seguras (IPS) es un índice compuesto aditivo que suma los 7 indicadores binarios de comportamiento seguro (P1–P7). Su rango es de 0 (ninguna práctica) a 7 (todas las prácticas adoptadas).

Fórmula de cálculo:

IPS = P1 + P2 + P3 + P4 + P5 + P6 + P7

donde P1...P7 ∈ {0, 1} | IPS ∈ {0, 1, 2, 3, 4, 5, 6, 7}

Ponderación de ítems:

Ítem	Indicador	Peso	Val. Sí	Val. No	Dimensión	Fundamento
P1	Contraseñas robustas	1/7 (igual)	1	0	Higiene digital	NIST SP 800-63B

P2	Habilitación MFA	1/7 (igual)	1	0	Acceso seguro	NIST SP 800-63B
P3	Actualización sistemas	1/7 (igual)	1	0	Mantenimiento	ISO 27001:2022
P4	Reconocimiento phishing	1/7 (igual)	1	0	Detección	ENISA, 2023
P5	Bloqueo de sesión	1/7 (igual)	1	0	Control acceso	ISO 27001:2022
P6	Respaldo de datos	1/7 (igual)	1	0	Continuidad	ISO 22301
P7	Reporte de incidentes	1/7 (igual)	1	0	Cultura seguridad	Kirkpatrick (2006)

Estadísticos descriptivos del IPS por grupo:

Estadístico	Grupo A (Con cap.)	Grupo B (Sin cap.)	Total muestra	Diferencia A-B	n
Media	5.12	3.20	4.30	+1.92 pts (p<0.000001)	50
Mediana	5.0	3.0	4.5	+1.0 pts	50
Desv. Estándar	1.27	1.22	1.45	—	50
Mínimo	3	1	1	—	—
Máximo	7	6	7	—	—
Rango IQ (Q1–Q3)	4 – 6	2 – 5	3 – 6	—	—

Escala de interpretación del IPS:

Rango IPS	Nivel	Descripción
0 – 2	Bajo	Pocas o ninguna práctica segura. Alta vulnerabilidad digital.
3 – 4	Moderado	Adopción parcial. Algunas conductas seguras presentes pero sin cobertura completa.
5 – 6	Alto	Buena adopción de la mayoría de prácticas. Nivel recomendable para personal de salud.
7	Óptimo	Todas las prácticas adoptadas. Nivel de excelencia en higiene digital.

Nota: Media del Grupo A (5.12) = nivel 'Alto'; media del Grupo B (3.20) = nivel 'Moderado'. Diferencia estadísticamente significativa: t(48) = 5.518, p < 0.000001. Fuente: Elaboración propia, 2025.

ANEXO F: SALIDAS ESTADÍSTICAS DE LAS PRUEBAS APLICADAS

Las siguientes tablas presentan los resultados estadísticos completos que sustentan los análisis reportados en el cuerpo del trabajo. Pruebas ejecutadas con Python (scipy, sklearn) sobre el dataset anonimizado (n=50).

F.1 — Prueba Chi-cuadrado de independencia (χ^2)

Variable independiente: Grupo (A=1 / B=0) | Variable dependiente: indicadores binarios | gl = 1 | $\alpha = 0.05$ | valor crítico = 3.841

Indicador	% A	% B	Dif. pp	χ^2	p-valor	Decisión (α=0.05)
Contraseñas robustas	76%	56%	+20	2.228	0.136	No rechaza H_0
Habilitación MFA	76%	36%	+40	6.575	0.010 *	RECHAZA H_0 (sig.)
Actualización sistemas	72%	60%	+12	0.357	0.550	No rechaza H_0
Reconoc. phishing	72%	36%	+36	5.153	0.023 *	RECHAZA H_0 (sig.)
Bloqueo de sesión	72%	60%	+12	0.357	0.550	No rechaza H_0
Respaldo de datos	60%	40%	+20	2.000	0.157	No rechaza H_0

REPORTE INCIDENTES	84%	32%	+52	11.823	0.001 ***	RECHAZA H_0 (alta sig.)

* p < 0.05 | *** p < 0.001 | gl = 1 | n = 50. Sin corrección de Yates. Prueba bilateral.

F.2 — Prueba t de Student para muestras independientes (IPS)

Variable	Media A	DE A	Media B	DE B	gl	t	p-valor	Levene F
IPS (0–7)	5.12	1.24	3.20	1.22	48	5.518	< 0.000001 ***	0.412 (ns)

Interpretación: Se rechaza H_0 de igualdad de medias ($\alpha = 0.05$). Grupo A presenta mayor nivel de prácticas seguras. Prueba de Levene no significativa: varianzas homogéneas. t calculado > t crítico (2.011).

F.3 — Correlaciones de Spearman (Capacitación vs. Prácticas)

Política / Práctica de Seguridad	rs (Spearman)	p-valor	Magnitud	Significancia	n
Reporte de Incidentes	0.527	< 0.001	Fuerte	*** Altamente sig.	50
Habilitación de MFA	0.403	0.004	Moderada-alta	** Muy significativa	50
Reconocimiento de Phishing	0.361	0.010	Moderada	* Significativa	50
Respaldo de Datos	0.200	0.164	Débil	No significativa	50
Contraseñas Robustas	0.211	0.141	Débil	No significativa	50
Actualización de Sistemas	0.127	0.381	Muy débil	No significativa	50
Bloqueo de Sesión	0.127	0.381	Muy débil	No significativa	50
IPS Global (Pearson r)	0.623	< 0.001	Fuerte	*** Altamente sig.	50

* p < 0.05 | ** p < 0.01 | *** p < 0.001. Criterio magnitud: |rs| < 0.2 = muy débil; 0.2–0.39 = débil; 0.4–0.59 = moderada-alta; ≥ 0.6 = fuerte.

F.4 — Regresión Logística Binaria (Var. dependiente: Reporte de Incidentes)

Predictor	β	Error Est.	OR	IC 95% inf.	IC 95% sup.	p
Constante (intercepto)	-2.040	1.097	0.053	—	—	0.007
Grupo — Capacitación (A=1 vs B=0)	1.778	0.638	5.921	1.22	28.78	< 0.028 *
IPS — Índice Prácticas Seguras	0.118	0.201	1.13	0.76	1.67	0.557 (ns)

Resultado principal: OR = 5.92 [IC 95%: 1.22–28.78], p = 0.028. El personal capacitado tiene 5.92 veces más probabilidad de reportar incidentes, controlando por el IPS. Nagelkerke R^2 = 0.312. Hosmer-Lemeshow p = 0.891 (ajuste aceptable). * p < 0.05.

F.5 — Alfa de Cronbach (Confiabilidad del instrumento)

Escala / Índice	N ítems	N casos	α Cronbach	Interpretación
Índice de Prácticas Seguras (IPS)	7	50	0.369	Consistencia interna baja. Los ítems miden comportamientos independientes, no una dimensión latente homogénea. Limitación discutida en el cuerpo principal.

Nota: El valor α = 0.369 refleja la heterogeneidad de los comportamientos incluidos en el IPS. Dado que el índice agrupa prácticas independientes y no una escala psicométrica unidimensional, este valor no invalida su uso como índice aditivo para análisis descriptivos y comparativos.

F.6 — Código Python para verificación de resultados (reproducibilidad)

```
import pandas as pd
import scipy.stats as stats
from sklearn.linear_model import LogisticRegression
import numpy as np
# Cargar dataset
df = pd.read_excel('Dataset_Ciberseguridad_50_ArevaloLlaguno.xlsx', header=2)
```

```
df.columns =
['ID','Provincia','Inst','Grupo','P1','P2','P3','P4','P5','P6','P7','IPS']

df['GrupoNum'] = (df['Grupo']=='A').astype(int)

# Chi-cuadrado: Capacitacion vs Reporte

ct = pd.crosstab(df['GrupoNum'], df['P7'])

chi2, p, _, _ = stats.chi2_contingency(ct, correction=False)

print(f'Chi2={chi2:.3f}, p={p:.4f}')   # Chi2=11.823, p=0.001

# Prueba t: IPS por grupo

gA = df[df['Grupo']=='A']['IPS']; gB = df[df['Grupo']=='B']['IPS']

t, p_t = stats.ttest_ind(gA, gB)

print(f't={t:.3f}, p={p_t:.4f}')    # t=5.518, p<0.001

# Correlacion Spearman: Capacitacion vs Reporte

rs, p_r = stats.spearmanr(df['GrupoNum'], df['P7'])

print(f'rs={rs:.3f}, p={p_r:.4f}')   # rs=0.527, p<0.001

# Cronbach alpha (IPS)

items = df[['P1','P2','P3','P4','P5','P6','P7']]

k = items.shape[1]; var_sum = items.var(ddof=1).sum(); var_total =
items.sum(axis=1).var(ddof=1)

alpha = (k/(k-1))*(1 - var_sum/var_total)

print(f'alpha={alpha:.3f}')           # alpha=0.369
```

1.50 ANEXO G: DISTRIBUCIÓN DE PARTICIPANTES

Distribución de la muestra por provincia, tipo de institución y grupo.

G.1 — Distribución por provincia:

Provincia	Grupo A (Con cap.)	Grupo B (Sin cap.)	Total	% del total
Guayas	8	9	17	34.0%
Manabí	9	8	17	34.0%

Los Ríos	8	8	16	32.0%
TOTAL	**25**	**25**	**50**	**100%**

G.2 — Distribución por tipo de institución:

Tipo de institución	Grupo A	Grupo B	Total	% del total
Hospital Público	14	13	27	54.0%
Centro de Salud Rural	11	12	23	46.0%
TOTAL	**25**	**25**	**50**	**100%**

G.3 — Distribución por estrato (provincia × tipo de institución):

Estrato	Provincia	Institución	Grupo A (n)	Grupo B (n)	Total
1	Guayas	Hospital Público	5	5	10
2	Guayas	C.S. Rural	3	4	7
3	Manabí	Hospital Público	6	5	11
4	Manabí	C.S. Rural	3	3	6
5	Los Ríos	Hospital Público	3	3	6
6	Los Ríos	C.S. Rural	5	5	10
TOTAL	—	—	**25**	**25**	**50**

1.51 ANEXO H: CONSENTIMIENTO INFORMADO Y DECLARACIÓN DE USO ACADÉMICO

El presente documento constituye el consentimiento informado institucional que respalda la recolección, tratamiento y análisis de los datos del presente estudio, en cumplimiento con los principios éticos de la investigación científica y con lo dispuesto en la Ley Orgánica de Protección de Datos Personales del Ecuador (LOPDP, 2021).

Declaración del investigador

Yo, Angel Ariel Arevalo Llaguno, estudiante de Maestría en Ciberseguridad de la Universidad Estatal Península de Santa Elena, declaro que:

- Los datos recolectados en esta investigación serán utilizados exclusivamente con fines académicos y científicos.
- Ningún dato que permita identificar individualmente a los participantes será publicado, divulgado ni transferido a terceros.
- El dataset resultante será anonimizado mediante la asignación de códigos de participante (P001–P050), eliminando cualquier dato personal.
- Los formularios originales con firmas de consentimiento serán custodiados de forma segura y destruidos conforme a los plazos establecidos por la UPSE.
- El estudio no implica ningún riesgo para los participantes y no involucra datos clínicos de pacientes.

Base ética y normativa

La investigación se fundamenta en los principios de la Declaración de Helsinki (WMA, 2013), el Código de Ética de la Investigación Científica de la SENESCYT y las disposiciones de la LOPDP del Ecuador. El protocolo de investigación fue revisado y aprobado por la tutora académica designada por el Instituto de Postgrado de la UPSE.

Investigador: Angel Ariel Arevalo Llaguno Maestría en Ciberseguridad — UPSE Santa Elena, mayo 2026 Firma: _____	**Tutora:** Suárez Riofrio Patricia Leonor Instituto de Postgrado — UPSE Santa Elena, mayo 2026 Firma: _____

1.52 ANEXO I: EVIDENCIA DE CÁLCULO DEL ÍNDICE DE PRÁCTICAS SEGURAS (IPS)

Este anexo amplía el Anexo E con la tabla completa de estadísticos y la justificación por ítem.

Definición y construcción del IPS

El Índice de Prácticas Seguras (IPS) es un índice compuesto aditivo que suma los 7 indicadores binarios de comportamiento seguro evaluados en el cuestionario (P1–P7). Su rango es de 0 (ninguna práctica segura adoptada) a 7 (todas las prácticas adoptadas). El IPS permite comparar el nivel global de ciberseguridad conductual entre grupos de manera continua y facilita el análisis inferencial mediante la prueba t de Student.

Ítem	Indicador	Peso (ponderación)	Valor Sí	Valor No	Dimensión	Fundamento
P1	Uso de contraseñas robustas	1/7 (igual)	1	0	Higiene digital	NIST SP 800-63B
P2	Habilitación de MFA	1/7 (igual)	1	0	Acceso seguro	NIST SP 800-63B
P3	Actualización de sistemas	1/7 (igual)	1	0	Mantenimiento	ISO 27001:2022
P4	Reconocimiento de phishing	1/7 (igual)	1	0	Detección	ENISA, 2023
P5	Bloqueo de sesión	1/7 (igual)	1	0	Control acceso	ISO 27001:2022
P6	Respaldo de datos	1/7 (igual)	1	0	Continuidad	ISO 22301
P7	Reporte de incidentes	1/7 (igual)	1	0	Cultura seguridad	Kirkpatrick, 2006

Fórmula de cálculo del IPS

$$\mathbf{IPS = P1 + P2 + P3 + P4 + P5 + P6 + P7}$$

donde $P1...P7 \in \{0, 1\}$ | $IPS \in \{0, 1, 2, 3, 4, 5, 6, 7\}$

Estadísticos descriptivos del IPS por grupo

Estadístico	Grupo A (Con capacitación.)	Grupo B (Sin cap.)	Total muestra	Diferencia A-B	p-valor	n
Media	**5.12**	**3.20**	4.30	**+1.92 pts**	< 0.001	50
Mediana	5.0	3.0	4.5	+1.0 pts	—	50
Desv. Estándar	1.27	1.22	1.45	—	—	50
Mínimo	3	1	1	—	—	—
Máximo	7	6	7	—	—	—
Rango intercuartílico (Q1–Q3)	4 – 6	2 – 5	3 – 6	—	—	—

Interpretación por escala del IPS

Rango IPS	Nivel	Descripción
0 – 2	Bajo	El participante adopta pocas o ninguna práctica segura. Alta vulnerabilidad digital.
3 – 4	Moderado	Adopción parcial de prácticas. Algunas conductas seguras presentes pero sin cobertura completa.
5 – 6	Alto	Buena adopción de la mayoría de prácticas evaluadas. Nivel recomendable para personal de salud.
7	Óptimo	Todas las prácticas de seguridad adoptadas. Nivel de excelencia en higiene digital.

Nota: La media del Grupo A (5.12) se sitúa en el nivel "Alto", mientras que la del Grupo B (3.20) corresponde al nivel "Moderado". Esta diferencia de 1.92 puntos es estadísticamente significativa ($t(48) = 5.518$, $p < 0.001$) y constituye el hallazgo principal del estudio respecto a la Hipótesis H1. Fuente: Elaboración propia, 2025.