



Modelos de Gestión en Privacidad de Datos de Salud Pública

Autoras: Shamary Poletth Valdospin Sánchez
Universidad Cesar Vallejo, **UCV**
p7002483915@ucvvirtual.edu.pe
Piura, Perú
<https://orcid.org/0000-0002-0526-4852>

Ingrid Angelina Soto Galarza
Universidad del Pacifico, **UP**
ingrid.soto@upacifico.edu.ec
Guayaquil, Ecuador
<https://orcid.org/0000-0003-1111-2836>

Elisa Amelia Cisneros Prieto
Tecnológico Universitario Argos, **TUA**
e_cisneros@tecnologicoargos.edu.ec
Guayaquil, Ecuador

Resumen

La digitalización acelerada del sector sanitario público en Ecuador ha incrementado los riesgos de vulnerabilidad en la gestión de datos sensibles. Este estudio tuvo como objetivo elaborar un modelo de gestión de política de privacidad para la consulta externa de usuarios en un hospital público ecuatoriano. Se implementó un enfoque cuantitativo transversal con alcance descriptivo-correlacional, aplicando un cuestionario estructurado a 300 usuarios seleccionados mediante muestreo probabilístico sistemático. Los resultados revelaron deficiencias significativas en todos los componentes evaluados: ninguno alcanzó el 50% de aprobación, siendo la gestión documental el más crítico 28,4%. El análisis factorial identificó tres componentes principales que explican el 88% de la varianza: gestión de accesos 34,2%, protección de datos 28,7% y cumplimiento normativo 25,1%. La satisfacción general de los usuarios fue de 3,2/10, evidenciando una crisis de confianza en el sistema actual. Se concluye que el modelo de gestión requiere una reestructuración integral basada en los tres componentes identificados para garantizar la protección efectiva de datos personales en el contexto hospitalario ecuatoriano.

Palabras clave: protección de datos; informática médica; gestión hospitalaria; privacidad; atención sanitaria.

Código de clasificación internacional: 1203.20 - Sistemas de control médico; 1203.12 - Bancos de datos.

Cómo citar este artículo:

Valdospin, S., Soto, I., & Cisneros, E. (2024). **Modelos de Gestión en Privacidad de Datos de Salud Pública.** *Revista Científica*, 9(34), 22-42, e-ISSN: 2542-2987. Recuperado de: <https://doi.org/10.29394/Scientific.issn.2542-2987.2024.9.34.2.41-62>

Fecha de Recepción:
18-05-2024

Fecha de Aceptación:
22-10-2024

Fecha de Publicación:
05-11-2024



Management Models in Public Health Data Privacy

Abstract

The accelerated digitalization of Ecuador's public health sector has increased vulnerability risks in sensitive data management. This study aimed to develop a privacy policy management model for outpatient users in a public hospital in Ecuador. A cross-sectional quantitative approach with descriptive-correlational scope was implemented, applying a structured questionnaire to 300 users selected through systematic probability sampling. Results revealed significant deficiencies in all evaluated components: none reached 50% approval, with document management being the most critical 28,4%. Factor analysis identified three main components explaining 88% of variance: access management 34,2%, data protection 28,7%, and regulatory compliance 25,1%. Overall user satisfaction was 3,2/10, evidencing a crisis of confidence in the current system. It is concluded that the management model requires comprehensive restructuring based on the three identified components to ensure effective personal data protection in the Ecuadorian hospital context.

Keywords: data protection; medical informatics; hospital management; privacy; health care.

International classification code: 1203.20 - Medical monitoring systems; 1203.12 - Data banks.

How to cite this article:

Valdospin, S., Soto, I., & Cisneros, E. (2024). **Management Models in Public Health Data Privacy.** *Revista Científica*, 9(34), 22-42, e-ISSN: 2542-2987. Retrieved from: <https://doi.org/10.29394/Scientific.issn.2542-2987.2024.9.34.2.41-62>

Date Received:
18-05-2024

Date Acceptance:
22-10-2024

Date Publication:
05-11-2024

Shamary Poleth Valdospin Sánchez; Ingrid Angelina Soto Galarza; Elisa Amelia Cisneros Prieto. Modelos de Gestión en Privacidad de Datos de Salud Pública. *Management Models in Public Health Data Privacy*.

H - R BY HUMAN - REAL 2412140372554

Revista Científica - Artículo Arbitrado - Registro nº: 295-14548 - pp. BA2016000002 - Vol. 9, Nº 34 - Noviembre-Enero 2024-2025 - pág. 41/62
e-ISSN: 2542-2987 - ISNI: 0000 0004 6045 0361



1. Introducción

La digitalización acelerada de los servicios de salud representa actualmente uno de los mayores desafíos en términos de gestión de la privacidad de datos personales. En el contexto latinoamericano, específicamente en Ecuador, la transformación digital del sector sanitario público ha evidenciado la necesidad imperante de establecer modelos de gestión robustos que garanticen la confidencialidad de la información médica. Los sistemas de salud modernos procesan diariamente grandes volúmenes de datos sensibles, desde historiales clínicos hasta resultados de pruebas diagnósticas, lo que aumenta exponencialmente los riesgos de vulnerabilidad informática (Díaz-Vélez, Peña, Galán-Rodas, Apolaya, Herrera-Añazco y Molinelli, 2023).

La gestión de la privacidad en el ámbito sanitario trasciende el mero cumplimiento normativo, constituyéndose en un elemento fundamental para la prestación de servicios de salud de calidad. De acuerdo con el informe de IBM, el sector salud experimenta los costes más elevados por brechas de seguridad, alcanzando los 10,93 millones de dólares por incidente en 2023, lo que representa un incremento del 53,3% desde 2020 (Cervera y Goussens, 2024). Esta realidad se agudiza particularmente en el sector público, donde las limitaciones presupuestarias y la falta de protocolos estandarizados incrementan la vulnerabilidad de los sistemas de información.

La literatura especializada destaca que la implementación de modelos estructurados de gestión de privacidad puede disminuir significativamente los riesgos asociados a incidentes de seguridad en entornos hospitalarios. Este impacto depende en gran medida de la integración efectiva de estos modelos con los procesos existentes y su adaptación al contexto local, considerando las complejidades inherentes al manejo de información sensible en el sector salud (Motti y Berkovsky, 2022a). En Ecuador, la ausencia de *frameworks* específicos para la gestión de la privacidad en el sector salud ha generado una brecha significativa entre las necesidades de protección de datos y las prácticas actuales (Salazar-Chalco y Campoverde-Molina, 2022).

Las consultas externas representan un punto crítico en la gestión de la



privacidad, dado que constituyen el primer nivel de contacto entre el sistema de salud y los usuarios. Los datos generados en estas interacciones requieren protecciones especiales, considerando que incluyen información demográfica, diagnósticos preliminares e historiales médicos completos (Alegre, et al., 2024). La gestión inadecuada de esta información no solo compromete la confidencialidad del paciente, sino que también puede afectar la calidad de la atención médica y la confianza en el sistema de salud público.

En el contexto ecuatoriano, la necesidad de establecer modelos de gestión de privacidad se ha vuelto más apremiante debido al incremento en la adopción de tecnologías digitales en el sector salud. Según lo informado por el Ministerio de Salud Pública (MSP, 2024a): el 94% de los centros de salud de primer nivel de la Red Pública de Salud ya cuentan con un registro único de historia clínica digital, con planes de extensión hacia los hospitales.

Esta amplia digitalización, junto con el nuevo Reglamento de la Ley de Protección de Datos, plantea desafíos éticos significativos para los profesionales médicos, quienes deben operar dentro de políticas de gobernanza claramente definidas, considerando que el paciente es el propietario de su información (Ministerio de Salud Pública, MSP, 2024b). Esta transformación digital, si bien mejora la eficiencia operativa, también aumenta la superficie de exposición a posibles violaciones de datos.

La evolución de las amenazas cibernéticas y la creciente sofisticación de los ataques dirigidos al sector salud demandan respuestas estructuradas y adaptativas. Los modelos de gestión de privacidad deben incorporar no solo aspectos técnicos sino también consideraciones éticas, legales y culturales propias del contexto ecuatoriano (Ordóñez, Correa y Correa, 2022a). La implementación efectiva de estos modelos requiere un enfoque holístico que considere tanto la infraestructura tecnológica como el factor humano.

Ante esta realidad, surge la siguiente pregunta de investigación: ¿Cómo desarrollar un modelo de gestión de política de privacidad que garantice la protección efectiva de los datos personales en la consulta externa de usuarios en hospitales públicos ecuatorianos, considerando el contexto actual de transformación digital y las



crecientes amenazas a la seguridad de la información?

El presente estudio tiene como objetivo elaborar un modelo de gestión de política de privacidad para la consulta externa de usuarios de un hospital público en Ecuador, considerando las particularidades del contexto local y las necesidades específicas de protección de datos en el ámbito sanitario. Este modelo busca establecer un marco de referencia que permita garantizar la confidencialidad de la información médica mientras se mantiene la eficiencia operativa y la calidad de la atención al paciente.

2. Metodología

El presente estudio se desarrolló bajo un enfoque cuantitativo transversal, método que, según Hernández-Sampieri y Mendoza (2018): resulta óptimo para analizar fenómenos en un momento específico del tiempo y establecer relaciones entre variables sin manipulación deliberada. Este enfoque sobre la gestión de datos en el sector salud ha sido respaldado por la Organización Panamericana de la Salud (OPS, 2022a): que en su documento sobre calidad de los servicios de salud en América Latina y el Caribe señala la importancia de establecer sistemas de información confiables y garantizar una adecuada gestión de datos en los servicios hospitalarios.

Como se evidencia en el documento, la calidad y seguridad en el manejo de la información constituyen elementos fundamentales para lograr una atención eficiente y efectiva, siendo necesario implementar políticas de protección de datos y mecanismos de control que aseguren la confidencialidad de la información de los pacientes.

2.1. Diseño y Alcance del Estudio

Se implementó un diseño no experimental transeccional descriptivo, siguiendo los lineamientos metodológicos propuestos por Creswell y Creswell (2023): quienes sostienen que este tipo de diseño permite obtener una fotografía precisa del fenómeno estudiado en un momento determinado. El alcance descriptivo-correlacional facilitó la caracterización de las variables de estudio: Modelo de Gestión

y Política de Privacidad, permitiendo establecer las relaciones existentes entre ambas.

2.2. Población y Muestra

La investigación se realizó en un hospital público de Guayaquil, Ecuador, durante el primer trimestre de 2024. La población estuvo constituida por 1,366 usuarios de consulta externa, cifra que representa el promedio mensual de pacientes atendidos en el período de estudio. Para la determinación del tamaño muestral se aplicó la fórmula para poblaciones finitas propuesta por García-García, Reding-Bernal y López-Alvarenga (2013): considerando los siguientes factores estadísticos: probabilidad de error tipo I (α) de 0,05, poder estadístico ($1-\beta$) de 0,80, y un error de estimación (d) determinado a partir de estudios previos similares.

Esto resultó en una muestra final de 300 usuarios. La selección de los participantes se realizó mediante un muestreo probabilístico sistemático, técnica respaldada por los estudios de Briones-Bermeo, Barreto-Rosado, Zambrano-Loor y Barreto-Rosado (2021a): en investigaciones similares del sector salud.

2.3. Instrumentos y Técnicas de Recolección de Datos

Para la recolección de datos se empleó un cuestionario estructurado como instrumento principal para el enfoque cuantitativo transversal, validado mediante el método Delphi con un panel de 12 expertos, alcanzando un índice de validez de contenido de 0,89, valor considerado óptimo según los criterios establecidos por Peters, Tran y Adam (2013). La selección de expertos para la validación Delphi se realizó siguiendo un proceso sistemático de tres fases como se puede apreciar en la tabla 1.

Tabla 1. Fases del Proceso de Evaluación de Expertos.

Fase	Actividades y Criterios
1. Fase de Identificación	<p>Base inicial: 25 candidatos potenciales.</p> <p>Criterios mínimos requeridos:</p> <ul style="list-style-type: none">• Grado académico de maestría o superior en áreas relacionadas.• Mínimo 10 años de experiencia en el sector salud.• Al menos 5 años de experiencia específica en gestión de

Artículo Original / Original Article

	<p>datos sanitarios.</p> <ul style="list-style-type: none"> Publicaciones académicas en el campo de la privacidad de datos.
2. Fase de Evaluación	<p>Aplicación del coeficiente de competencia experta (K):</p> <ul style="list-style-type: none"> Autoevaluación de conocimiento sobre el tema (Ka) Análisis de fuentes de argumentación (Kc) <p>Criterio de selección: $K \geq 0,8$</p> <p>Distribución final del panel:</p> <ul style="list-style-type: none"> 5 especialistas en sistemas de información sanitaria. 4 expertos en protección de datos y privacidad. 3 profesionales de gestión hospitalaria.
3. Fase de Compromiso	<ul style="list-style-type: none"> Confirmación de disponibilidad para tres rondas de evaluación. Firma de acuerdos de confidencialidad. Establecimiento de cronograma de participación.

Fuente: Las Autoras (2024).

Es notable que el proceso de selección implementó un enfoque riguroso que equilibró experiencia práctica y formación académica. Los requisitos específicos y el coeficiente de competencia experta ($K \geq 0,8$) garantizaron un panel de alta calidad, mientras que su composición multidisciplinaria aseguró una evaluación integral del modelo de gestión de privacidad en el contexto sanitario. El establecimiento formal de compromisos refuerza la validez metodológica de la investigación.

Los criterios de inclusión y exclusión para los participantes del estudio se definieron de la siguiente manera:

- Criterios de inclusión: Usuarios mayores de 18 años; Mínimo tres consultas previas en el último año; Capacidad para comprender y firmar el consentimiento informado; y Usuarios que hayan tenido al menos una interacción con el sistema digital de historia clínica
- Criterios de exclusión: Pacientes en situación de emergencia; Usuarios que no completaron el 100% del cuestionario; Personal del hospital o familiares directos; Pacientes con deterioro cognitivo documentado; y Usuarios que no aceptaron participar voluntariamente.

El cuestionario se estructuró en dos dimensiones principales, utilizando una

escala Likert de 5 puntos:

- 1). Modelo de Gestión (25 ítems) que evaluó: Procesos de control de acceso; Sistemas de protección de datos; Protocolos de seguridad; Gestión documental; y Capacitación del personal.
- 2). Política de Privacidad (20 ítems) que evaluó: Normativas internas; Cumplimiento legal; Protocolos de confidencialidad; Manejo de consentimientos; y Gestión de derechos de usuarios.

La confiabilidad del instrumento se determinó mediante el coeficiente Alpha de Cronbach, obteniendo un valor de 0,92, que para Bastidas (2023): indica una alta consistencia interna.

2.4. Procedimiento

La recolección de datos se realizó durante un período de 45 días, previa obtención de las autorizaciones institucionales correspondientes y la aprobación del Comité de Ética del hospital (Ministerio de Salud Pública, OPS, 2024c, 2024d). Todos los participantes firmaron un consentimiento informado, siguiendo los protocolos éticos establecidos por Sánchez (2016a): para investigaciones en entornos hospitalarios.

2.5. Análisis de Datos

El procesamiento y análisis de datos se realizó utilizando el software *IBM SPSS Statistics*. Se aplicaron técnicas de estadística descriptiva e inferencial, incluyendo:

- Análisis de frecuencias y medidas de tendencia central.
- Pruebas de correlación de Pearson para establecer relaciones entre variables.
- Análisis factorial confirmatorio para validar las dimensiones del modelo propuesto.



El análisis siguió los procedimientos recomendados por Álvarez (2007a): para estudios en gestión de la salud pública, considerando aspectos cuantitativos de recopilación y procesamiento estadístico de datos para evaluar la implementación de políticas sanitarias. Se emplearon técnicas de estadística descriptiva para analizar frecuencias y medidas de tendencia central, pruebas de correlación de Pearson para establecer relaciones entre variables, y análisis factorial confirmatorio para validar las dimensiones del modelo propuesto.

Este enfoque permitió examinar la gestión actual de privacidad, las necesidades de protección de datos y las expectativas sobre políticas de privacidad, siguiendo las recomendaciones sobre investigación cuantitativa en el sector salud que enfatizan la importancia de contar con evidencia empírica para la toma de decisiones en políticas públicas de salud. El análisis se complementó con la revisión de documentos oficiales y marcos normativos vigentes, siguiendo los lineamientos metodológicos para estudios de implementación en sistemas de salud.

2.6. Consideraciones Éticas

La investigación se desarrolló bajo los principios éticos establecidos en la Declaración de Helsinki y las normativas locales de investigación en salud. Se garantizó la confidencialidad de los participantes mediante la codificación de datos y el almacenamiento seguro de la información, siguiendo los protocolos de protección de datos establecidos por Enríquez (2017). El estudio contó con la aprobación del Comité de Ética Institucional y el Consejo Científico del hospital, cumpliendo con todos los requisitos de investigación en seres humanos establecidos por la legislación ecuatoriana vigente.

3. Resultados

El análisis de los datos recolectados en el hospital público de Guayaquil durante el primer trimestre de 2024 se realizó a partir de la aplicación de un cuestionario estructurado a 300 usuarios de consulta externa, evaluando las variables de Modelo de Gestión y Política de Privacidad.

3.1. Instrumento de evaluación

El cuestionario aplicado constó de 45 ítems (25 + 20) distribuidos entre estas dos dimensiones principales, cada uno evaluado mediante una escala Likert de 5 puntos, donde 1 representa “Totalmente en desacuerdo” y 5 “Totalmente de acuerdo” (tabla 1).

Tabla 1. Estructura del Instrumento de Evaluación.

Dimensión	Componentes Evaluados	Número de Ítems
Modelo de Gestión	- Procesos de control de acceso	5
	- Sistemas de protección de datos	5
	- Protocolos de seguridad	5
	- Gestión documental	5
	- Capacitación del personal	5
	Total	25
Política de Privacidad	- Normativas internas	4
	- Cumplimiento legal	4
	- Protocolos de confidencialidad	4
	- Manejo de consentimientos	4
	- Gestión de derechos de usuarios	4
	Total	20

Fuente: Los Autores (2024).

Esta estructura permitió una evaluación comprehensiva tanto de los aspectos operativos (Modelo de Gestión) como normativos (Política de Privacidad) del manejo de información sensible en el hospital, generando métricas cuantitativas precisas para la toma de decisiones y la implementación de mejoras en el sistema. Este método facilitó la identificación de áreas críticas, permitiendo desarrollar estrategias específicas para fortalecer la protección y confidencialidad de la información clínica, alineadas con los estándares de seguridad y las normativas vigentes del sector sanitario.

3.1. Evaluación del Modelo de Gestión Actual

La tabla 2 presenta el nivel de cumplimiento en los componentes del Modelo de Gestión, basado en un análisis de respuestas favorables (niveles 4 y 5 en la escala Likert) de los 300 usuarios encuestados.

Tabla 2. Nivel de Cumplimiento en Componentes del Modelo de Gestión.

Componente Evaluado	Respuestas Favorables*	Porcentaje (%)
Procesos de control de acceso	136	45,3
Sistemas de protección	116	38,7
Protocolos de seguridad	96	32,1
Gestión documental	85	28,4

Artículo Original / Original Article

Capacitación verificada	124	41,2
*Respuestas en niveles 4 y 5 de la escala Likert		

Fuente: Los Autores (2024).

Los resultados revelan que ningún componente alcanza el 50% de aprobación, siendo los procesos de control de acceso el aspecto mejor evaluado con 45,3% (136 respuestas favorables), seguido por la capacitación verificada con 41,2% (124 respuestas), sistemas de protección con 38,7% (116 respuestas), protocolos de seguridad con 32,1% (96 respuestas), y finalmente la gestión documental como el componente peor evaluado con solo 28,4% (85 respuestas favorables).

Estos porcentajes indican deficiencias significativas en todos los aspectos evaluados del modelo de gestión actual, sugiriendo la necesidad de una reestructuración integral del sistema, con especial atención en la gestión documental y los protocolos de seguridad que muestran los niveles más bajos de cumplimiento.

3.2. Análisis de las Políticas de Privacidad

El gráfico 1 muestra la evaluación de los diferentes componentes de la Política de Privacidad en una escala del 1 al 5, donde el “Cumplimiento legal” obtiene la valoración más alta con 3,1 puntos, seguido por el “Manejo de consentimientos” con 2,9 puntos y las “Normativas internas” con 2,8 puntos. Los componentes con menor valoración son la “Gestión de derechos” con 2,7 puntos y los “Protocolos de confidencialidad” con 2,6 puntos.

Gráfico 1. Evaluación de Componentes de Política de Privacidad.



Fuente: Los Autores (2024).

Estos resultados son preocupantes ya que ningún componente supera los 3,1 puntos de 5 posibles, lo que indica deficiencias significativas en todos los aspectos

de la política de privacidad, siendo particularmente crítica la situación de los protocolos de confidencialidad que obtienen la puntuación más baja. La visualización en barras horizontales permite comparar fácilmente las diferencias entre componentes y evidencia la necesidad de mejoras sustanciales en todo el sistema de gestión de privacidad.

3.3. Análisis de Satisfacción de Usuarios

La evaluación de satisfacción de los usuarios se realizó mediante cuatro dimensiones clave, utilizando una escala de 1 a 10, donde 10 representa la máxima satisfacción. Los resultados revelan niveles críticos de insatisfacción: el nivel de confianza en el manejo de datos alcanzó apenas un 3,4/10, la facilidad de acceso a información obtuvo 3,3/10, la claridad de los procesos logró un 3,1/10, y la percepción de seguridad registró la puntuación más baja con 3,0/10. El promedio general de satisfacción fue de 3,2/10, lo cual es consistente con los bajos niveles de cumplimiento observados en el modelo de gestión (tabla 2) y la deficiente valoración de los componentes de política de privacidad (gráfico 1).

Estos resultados evidencian una crisis significativa en la confianza de los usuarios hacia el sistema actual y respaldan la urgente necesidad de implementar mejoras sustanciales en los protocolos de privacidad y seguridad del hospital público estudiado, especialmente en aspectos relacionados con la percepción de seguridad y la claridad de los procesos, que son los componentes peor evaluados.

3.4. Análisis Factorial

Para validar la estructura del modelo de gestión y determinar sus componentes principales, se realizó un análisis factorial exploratorio empleando el método de componentes principales con rotación Varimax. La idoneidad de los datos para este análisis fue confirmada mediante la prueba de Kaiser-Meyer-Olkin (KMO), que arrojó un valor de 0,82, indicando una adecuada correlación entre variables, y la prueba de esfericidad de Bartlett resultó significativa ($p < 0,001$), confirmando que la matriz de correlaciones no es una matriz de identidad.

El análisis identificó tres factores principales que explican el 88% de la



varianza total: la Gestión de Accesos y Autenticación (34,2%), la Protección de Datos Sensibles (28,7%), y el Cumplimiento Normativo y Auditoría (25,1%). La robustez de estos factores fue validada mediante el coeficiente Alpha de Cronbach, obteniendo valores de 0,89, 0,90 y 0,92 respectivamente para cada factor, lo que indica una alta consistencia interna en todas las dimensiones.

Estos resultados se alinean con los bajos niveles de satisfacción reportados en la sección 3,3 y las deficiencias identificadas en las políticas de privacidad (gráfico 1), proporcionando una base empírica sólida para el desarrollo de un nuevo modelo de gestión que aborde las necesidades específicas del contexto hospitalario público ecuatoriano, con especial énfasis en los tres factores identificados que explican la mayor parte de la variabilidad en la gestión de la privacidad de datos.

4. Discusión

Los hallazgos del presente estudio revelan desafíos significativos en la gestión de la privacidad de datos en el contexto hospitalario público ecuatoriano, particularmente en el área de consulta externa. El análisis de los resultados permite establecer comparaciones relevantes con la literatura existente y proponer implicaciones prácticas para la mejora de los sistemas actuales.

4.1. Análisis del Modelo de Gestión Actual

Los esfuerzos por fortalecer los sistemas de información para la salud en Ecuador, como parte del Plan de Acción 2024-2030 respaldado por la OPS, responden a la necesidad de mejorar la gestión y gobernanza de datos en el sector. Si bien se han logrado avances significativos en la implementación de estándares de interoperabilidad y en la digitalización de centros de atención primaria, aún existen desafíos importantes en la extensión del registro único de historia clínica digital hacia los hospitales.

Esto coincide con el compromiso de fortalecer los sistemas de información para garantizar una atención más eficiente y centrada en el paciente, reconociendo que la data se ha convertido en un instrumento crucial para la toma de decisiones (Ministerio de Salud Pública, MSP, 2024e).



Un aspecto crítico identificado en el estudio es la deficiente gestión documental digital en el ámbito sanitario ecuatoriano. Como señala Álvarez (2007b): el personal médico y administrativo presenta importantes carencias en su formación sobre seguridad informática y manejo de datos digitales. Esta brecha de conocimiento incrementa significativamente la vulnerabilidad del sistema, exponiendo la información sensible de los pacientes a riesgos como filtraciones, pérdidas o accesos no autorizados debido a errores prevenibles en la manipulación de dispositivos y sistemas informáticos.

La formación continua del personal sanitario en materia de protección y privacidad de datos constituye un elemento crítico en la arquitectura de seguridad hospitalaria. La investigación demuestra que los programas de capacitación más exitosos son aquellos que se diseñan considerando el contexto específico de cada institución y se integran orgánicamente con los flujos de trabajo existentes (Motti y Berkovsky, 2022b). Este abordaje integral no solo minimiza las vulnerabilidades en el manejo de información sensible, sino que además genera un impacto positivo en la percepción de confiabilidad institucional por parte de los pacientes.

4.2. Evaluación de las Políticas de Privacidad

La evaluación de las políticas de privacidad en el sector salud ecuatoriano revela una situación que requiere atención inmediata. Como señalan Ordóñez, Correa y Correa (2022b): en el contexto de la emergencia sanitaria se evidenció la carencia de políticas públicas en materia de protección de datos personales, especialmente en el ámbito de la salud.

El marco regulatorio ecuatoriano carece de protección para datos sanitarios, limitándose a la seguridad digital para menores. Esta ausencia crea un vacío en los protocolos de gestión de información médica tanto pública como privada. La falta de lineamientos y estrategias de concientización deja vulnerables los datos de salud pública, demostrando la necesidad urgente de políticas integrales.

La protección de la confidencialidad de la información en el sector salud resulta especialmente relevante, como lo señala la Organización Panamericana de la Salud (OPS, 2002b): en su documento sobre calidad de los servicios de salud.



Particularmente, cuando se trata de datos sensibles como historiales médicos, resultados de pruebas y datos personales, que son altamente valiosos y requieren medidas específicas de protección.

Los expedientes médicos contienen información confidencial que requiere protecciones extraordinarias debido a su impacto en la vida de los pacientes. La exposición inadecuada puede causar discriminación y vulnerar derechos fundamentales, comprometiendo la privacidad e integridad psicosocial. Por ello, proteger esta información es un imperativo ético y legal del sistema sanitario.

4.3. Satisfacción de Usuarios y Confianza en el Sistema

El índice global de satisfacción de 3,2/10 refleja una crisis de confianza en el sistema actual. Este resultado es consistente con los hallazgos de Bastidas (2023b): quienes documentaron niveles similares de insatisfacción en usuarios de servicios de salud pública respecto a la protección de sus datos personales. La baja percepción de seguridad (3,0/10) sugiere la necesidad urgente de implementar medidas correctivas, alineándose con las recomendaciones de Sánchez (2016b): sobre la importancia de la transparencia en la gestión de datos sanitarios.

4.4. Implicaciones para la Práctica

Los tres factores identificados en el análisis factorial (Gestión de Accesos, Protección de Datos y Cumplimiento Normativo) proporcionan un marco estructural para el desarrollo de un nuevo modelo de gestión. Esta estructura tripartita coincide con el modelo propuesto por Briones-Bermeo, Barreto-Rosado, Zambrano-Loor y Barreto-Rosado (2021b): aunque nuestros hallazgos sugieren una mayor relevancia del componente de gestión de accesos (34,2% de varianza explicada).

4.5. Limitaciones y Futuras Líneas de Investigación

Es necesario reconocer las limitaciones metodológicas de esta investigación. La principal restricción radica en que el estudio se circunscribió a un solo centro hospitalario del sistema público ecuatoriano, lo cual podría afectar la extrapolación de los hallazgos a otros contextos institucionales. Para fortalecer la validez externa de



los resultados, las investigaciones subsecuentes deberían ampliar el alcance del estudio para incluir una muestra representativa de diversos hospitales tanto públicos como privados del sistema nacional de salud.

Adicionalmente, el enfoque transversal del estudio no permite evaluar la evolución temporal de las variables analizadas. Se recomienda realizar estudios longitudinales que permitan valorar el impacto de las mejoras implementadas en el tiempo. Las implicaciones de estos hallazgos sugieren la necesidad de:

1. Desarrollar programas de capacitación intensiva en protección de datos para el personal sanitario.
2. Implementar sistemas de auditoría regular de los protocolos de privacidad.
3. Establecer mecanismos de retroalimentación continua con los usuarios.
4. Actualizar las políticas de privacidad según estándares internacionales.
5. Fortalecer los sistemas de gestión documental y control de accesos.

5. Conclusiones

El modelo de gestión de política de privacidad para la consulta externa en hospitales públicos de Ecuador requiere una reestructuración integral que garantice la protección efectiva de los datos personales de los usuarios. La evaluación sistemática realizada revela que las prácticas actuales son insuficientes para asegurar la confidencialidad y el manejo adecuado de la información sensible en el entorno sanitario.

La investigación ha permitido identificar una brecha significativa entre los estándares requeridos y la realidad operativa en la gestión de la privacidad. El índice de satisfacción de 3,2/10 refleja una crisis de confianza que demanda acciones inmediatas para salvaguardar la integridad de la información personal en el sistema de salud público.

El análisis factorial ha develado tres pilares fundamentales para la construcción de un modelo de gestión efectivo: la gestión de accesos y autenticación, la protección de datos sensibles, y el cumplimiento normativo y auditoría. Esta



estructura tripartita constituye la base para el desarrollo de políticas de privacidad más robustas y adaptadas al contexto hospitalario ecuatoriano.

La aplicación práctica de estos hallazgos sugiere la necesidad de implementar un sistema integrado de gestión de privacidad que incluya protocolos estandarizados, capacitación continua del personal y mecanismos de auditoría regular. La transformación digital del sector salud demanda que estas medidas sean flexibles y adaptables a las nuevas tecnologías y amenazas emergentes.

Entre las limitaciones del estudio, debe considerarse que la investigación se realizó en un único centro hospitalario y en un momento específico del tiempo. No obstante, la metodología empleada y los instrumentos desarrollados proporcionan una base sólida para futuras investigaciones en otros centros de salud del sistema público ecuatoriano.

Las líneas futuras de investigación deberían enfocarse en: El desarrollo de indicadores de desempeño específicos para la gestión de privacidad en salud, La evaluación del impacto de las tecnologías emergentes en la protección de datos sanitarios, El análisis comparativo de modelos de gestión de privacidad entre diferentes instituciones de salud y El estudio de la relación entre la privacidad de datos y la calidad de atención al paciente.

La implementación de un modelo de gestión de política de privacidad robusto y efectivo no solo mejorará la protección de datos personales, sino que también fortalecerá la confianza de los usuarios en el sistema de salud público, contribuyendo así a una mejor calidad de atención sanitaria en Ecuador.

6. Referencias

- Alegre, V., Álvarez, M., Bianchini, A., Buedo, P., Campi, N., Cristina, M., ... Luna, F. (2024). **Salud digital en América Latina: legislación actual y aspectos éticos**. *Revista Panamericana de Salud Pública*, 48(31), 1-9, e-ISSN: 1680-5348. Recuperado de: <https://doi.org/10.26633/RPSP.2024.40>
- Álvarez, R. (2007). **Estadística aplicada a las ciencias de la salud**. ISBN: 978-84-7978-823-0. España: Ediciones Díaz de Santos.
- Bastidas, S. (2023a,b). **Análisis de riesgo en la seguridad de los datos médicos**



mediante la utilización de la norma ISO/IEC 27110:2021. Tesis. Quito, Ecuador: PUCE.

Briones-Bermeo, N., Barreto-Rosado, M., Zambrano-Loor, L., & Barreto-Rosado, M. (2021a,b). **Sistema de salud del Ecuador. Comparativo de las políticas públicas a nivel organizacional y su efecto en los servicios de salud.** *Dominio de las Ciencias*, 7(1), 32-49, e-ISSN: 2477-8818. Ecuador: Polo de Capacitación, Investigación y Publicación.

Cervera, A., & Goussens, A. (2024). **Ciberseguridad y uso de las TIC en el Sector Salud.** *Atención Primaria*, 56(3), 1-7, e-ISSN: 0212-6567. Recuperado de: <https://doi.org/10.1016/j.aprim.2023.102854>

Creswell, J., & Creswell, J. (2023). **Research design: Qualitative, quantitative, and mixed methods approaches.** 6th edition, ISBN: 9781071817940. United States: SAGE Publications, Inc.

Díaz-Vélez, C., Peña, R., Galán-Rodas, E., Apolaya, M., Herrera-Añazco, P., & Molinelli, F. (2023). **Retos y perspectivas de las agencias de evaluación de tecnologías en salud en el Perú.** *Revista del Cuerpo Médico Hospital Nacional Almanzor Aguinaga Asenjo*, 16(2), 1-12, e-ISSN: 2227-4731. Perú: Cuerpo Médico Hospital Nacional Almanzor Aguinaga Asenjo.

Enríquez, L. (2017). **Paradigmas de la protección de datos personales en Ecuador. Análisis del proyecto de Ley Orgánica de Protección a los Derechos a la Intimidad y Privacidad sobre los Datos Personales.** *Revista de Derecho*, (27), 43-61, e-ISSN: 1390-2466. Ecuador: Universidad Andina Simón Bolívar.

García-García, J., Reding-Bernal, A., & López-Alvarenga, J. (2013). **Cálculo del tamaño de la muestra en investigación en educación médica.** *Investigación en educación médica*, 2(8), 217-224, e-ISSN: 2007-5057. México: Universidad Nacional Autónoma de México, Facultad de Medicina.

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

Motti, V., & Berkovsky, S. (2022a,b). **Healthcare Privacy.** In Knijnenburg, B., Page,



X., Wisniewski, P., Lipford, H., Proferes, N., Romano, J. (eds). *Modern Socio-Technical Perspectives on Privacy*. ISBN: 978-3-030-82786-1. (pp. 203-231). Cham, Suiza: Springer.

MSP (2024a,b,e). **Ecuador apoya el Plan de Acción de la OPS para fortalecer los sistemas de información en salud**. Quito, Ecuador: Ministerio de Salud Pública.

MSP (2024c). **Aprobación de Comités de Ética de Investigación en Seres Humanos**. Quito, Ecuador: Ministerio de Salud Pública.

MSP (2024d). **Aprobación de Comités de Ética Asistenciales para la Salud**. Quito, Ecuador: Ministerio de Salud Pública.

OPS (2002a,b). **Calidad de los servicios de salud en América Latina y el Caribe: Desafíos para la enfermería**. Estados Unidos: Organización Panamericana de la Salud.

Ordóñez, L., Correa, L., & Correa, A. (2022a,b). **Políticas públicas y protección de datos personales en Ecuador: reflexiones desde la emergencia sanitaria**. *Estado & Comunes*, 2(15), 77-97, e-ISSN: 2477-9245. Recuperado de: https://doi.org/10.37228/estado_comunes.v2.n15.2022.270

Peters, D., Tran, N., & Adam, T. (2013). *Implementation Research in Health: A Practical Guide*. ISBN: 978-92-4-150621-2. Switzerland: World Health Organization.

Salazar-Chalco, J., & Campoverde-Molina, M. (2022). **Detección de vulnerabilidades informáticas en estaciones de trabajo: Caso de estudio Hospital de Especialidades José Carrasco Arteaga**. *Polo del Conocimiento*, 7(4), 446-465, e-ISSN: 2550-682X. Ecuador: Casa Editora del Polo.

Sánchez, M. (2016a,b). **Protocolos éticos para resolver situaciones problemáticas**. Ecuador: Ministerio de Salud Pública.

Shamary Poleth Valdospin Sánchez

e-mail: p7002483915@ucvvirtual.edu.pe



Nacida en Guayaquil, Ecuador el 2 de agosto del año 1992. Licenciada en Enfermería por la Universidad Católica de Santiago de Guayaquil (UCSG) de Ecuador; Maestra en Gestión de los Servicios de la Salud por la Universidad César Vallejo (UCV) de Perú; Certificación de Formador de Formadores por parte de la empresa Ser más Consultoría y coaching; actualmente presto Servicios al Hospital General Guasmo Sur, perteneciente al Ministerio de Salud Pública (MSP).

Ingrid Angelina Soto Galarzae-mail: ingrid.soto@upacifico.edu.ec

Nacida en Guayaquil, Ecuador el 11 de agosto del año 1976. Ingeniera en Estadística Informática por la Universidad Politécnica del Litoral (ESPOL); Máster en Investigación de Mercados y Máster en Productividad y la calidad de la misma Universidad (ESPOL); Máster en Administración de empresas con Mención en Marketing y Máster en Finanzas y economía de la Universidad Estatal de Guayaquil (UEG); Empresaria en Bienes Raíces desde hace más de 30 años; fui Gerente de varias empresas de producción; Docente en la Universidad del Pacífico (UP); y en el Instituto Superior Tecnológico Humane (ISTH).

Elisa Amelia Cisneros Prieto

e-mail: e_cisneros@tecnologicoargos.edu.ec



Nacida en Guayaquil, Ecuador el 24 de noviembre del año 1979. Ingeniera en Sistemas Computacionales de la Universidad Católica de Santiago de Guayaquil (UCSG); Máster en Administración de empresas con Mención en Marketing de la Universidad Estatal de Guayaquil (UEG); fui jefe del Departamento de sistemas de una multiempresa; adicionalmente fui Directora de la Facultad de tecnología a nivel universitario; Docente en el Tecnológico Universitario ARGOS.