REVISTA ECUATORIANA DE DESARROLLO SOCIAL Y AMBIENTAL
Julio - Septiembre, 2026 | Vol. 1 | Núm. 3
ISSN: 3151-8303

Modelo de buenas prácticas para seguridad de información en Hospitales Nivel II

Model of Good practices for information security in Level II Hospitals

Jorge Luis Carranza Lujan
1 Universidad Nacional del Santa; La Caleta - Perú;
jcarranzal@hotmail.com
https://orcid.org/0009-0006-9524-4973

Enviado: 11/06/2026 **Aceptado:** 29/06/2026 **Publicado:** 03/07/2026

Tipo de Investigación: Artículo Original **Páginas:** 1 - 9

DOI: https://doi.org/10.66646/redsa-2026/3zv24c78

Conflicto de Intereses Ninguno que declarar.

Correspondecia: **Jorge Luis Carranza Lujan**
Universidad Nacional del Santa; La Caleta - Perú;
jcarranzal@hotmail.com

RESUMEN

La protección de la información en hospitales públicos plantea un desafío importante en entornos donde los recursos tecnológicos son limitados y las políticas formales son escasas. Este estudio tuvo como objetivo desarrollar un modelo de buenas prácticas para gestionar de manera eficaz la seguridad de la información en el Hospital Nivel II La Caleta de Chimbote, Perú. A través de un enfoque cuantitativo, descriptivo-propositivo y un diseño no experimental transversal, se realizaron encuestas y entrevistas a una muestra de 30 empleados de las áreas de TI, administrativa y asistencial, junto con el análisis de registros institucionales del año 2024. Los hallazgos revelaron un nivel de madurez que varía de bajo a medio en cuanto a seguridad de la información: el 80% del personal desconocía la existencia de políticas formales, el 95% reportó la falta de metodologías para la gestión de riesgos y de simulacros de contingencia, el 100% de los dispositivos no contaba con un antivirus actualizado y se registraron 145 incidentes de seguridad, siendo el malware la principal amenaza (32,4%), con períodos de inactividad que alcanzaron hasta 35 horas en módulos críticos. Ante esta situación, se propuso un modelo estructurado que se alinea con la norma ISO/IEC 27001, el cual integra políticas de seguridad, controles técnicos, gestión de riesgos y programas de capacitación continua. Se concluye que implementar este modelo permitirá proteger la confidencialidad, integridad y disponibilidad de la información clínica y administrativa, fortaleciendo así la continuidad operativa del hospital.

Palabras clave:
ISO/IEC 27001; Tecnologia.

ABSTRACT

Protecting information in public hospitals presents a significant challenge in environments where technological resources are limited and formal policies are scarce. This study aimed to develop a best practice model for effectively managing information security at the La Caleta Level II Hospital in Chimbote, Peru. Through a quantitative, descriptive-propositive approach and a non-experimental, cross-sectional design, surveys and interviews were conducted with a sample of 30 employees from the IT, administrative, and support areas, along with an analysis of institutional records from 2024. The findings revealed a low to medium level of maturity in information security: 80% of staff were unaware of the existence of formal policies, 95% reported a lack of risk management methodologies and contingency drills, 100% of devices lacked updated antivirus software, and 145 security incidents were recorded, with malware being the main threat (32.4%), resulting in downtime of up to 35 hours in critical modules. In response to this situation, a structured model aligned with the ISO/IEC 27001 standard was proposed, integrating security policies, technical controls, risk management, and ongoing training programs. It is concluded that implementing this model will protect the confidentiality, integrity, and availability of clinical and administrative information, thus strengthening the operational continuity of the hospital.

Keywords:
ISO/IEC 27001; Tecnology.

INTRODUCCIÓN

La protección de la información es un componente esencial en la administración de organizaciones que manejan datos sensibles, siendo los centros de salud pública uno de los ámbitos más expuestos a amenazas cibernéticas y a la pérdida de información. En América Latina, la mayoría de los hospitales públicos no disponen de políticas formalizadas que regulen la salvaguarda de sus activos informáticos, una situación que se complica debido a limitaciones presupuestarias, tecnología desactualizada y una cultura organizacional débil en cuestiones de seguridad. Los hospitales de nivel II manejan de manera simultánea datos clínicos, administrativos y operativos de alta relevancia, cuya pérdida, alteración o divulgación no autorizada puede poner en riesgo la continuidad del servicio y la privacidad de los pacientes.

El Hospital La Caleta de Chimbote, un establecimiento público de nivel II, se enfrenta a esta problemática. Su infraestructura tecnológica, conformada por alrededor de 180 computadoras interconectadas en una arquitectura cliente-servidor, experimenta con frecuencia incidentes de seguridad, incluyendo infecciones de malware, accesos no permitidos, pérdida o corrupción de datos y caídas prolongadas de sistemas críticos, habiendo registrado más de 4,320 interrupciones en el último año. Esta situación evidencia la falta de un Sistema de Gestión de Seguridad de la Información (SGSI) formalmente establecido, así como de mecanismos sistemáticos para la gestión de riesgos y planes de continuidad del negocio. La norma internacional ISO/IEC 27001 prescribe los requisitos para la implementación de un SGSI, ofreciendo un marco de referencia reconocido a nivel global para la protección de la información a través de controles técnicos, organizacionales y humanos; sin embargo, su adopción en el sector hospitalario público peruano aún es incipiente.

Ante este contexto, la investigación se justifica operativamente por la necesidad apremiante de disminuir la frecuencia de eventos de seguridad que afectan la atención al paciente y la gestión institucional, y académicamente por la falta de modelos adaptados a las realidades de los hospitales públicos de nivel II en el contexto nacional. La principal aportación de este trabajo radica en la presentación de un modelo de buenas prácticas específicamente diseñado para este tipo de instituciones, el cual integra políticas de seguridad, controles técnicos, gestión de riesgos y programas de sensibilización del personal, alineándose con los dominios de la norma ISO/IEC 27001. A diferencia de estudios anteriores que utilizan marcos generales o más complejos, este modelo toma en cuenta las limitaciones presupuestarias, el nivel de madurez tecnológica y las características operativas únicas de los hospitales públicos peruanos de nivel II, ofreciendo una solución viable, escalable y replicable en instituciones similares de la región.

En este contexto, la presente investigación se planteó los siguientes objetivos:

Objetivo general:

Proponer un modelo de buenas prácticas para gestionar de manera eficiente la seguridad de la información en el Hospital Nivel II La Caleta de Chimbote.

Objetivos específicos:

- Diagnosticar el estado actual de la seguridad de la información en el Hospital Nivel II La Caleta, identificando incidentes,

vulnerabilidades y la infraestructura tecnológica disponible.

- Identificar las brechas de cumplimiento respecto a los dominios de la norma ISO/IEC 27001 que son aplicables a hospitales públicos de nivel II.
- Diseñar un modelo de buenas prácticas que combine políticas, controles técnicos, gestión de riesgos y métodos de capacitación orientados a reforzar la seguridad de la información institucional.

METODOLOGÍA

Diseño de investigación

El estudio utilizó un enfoque cuantitativo de tipo aplicado, con un nivel descriptivo-propositivo y un diseño transitorio no experimental. Se considera no experimental ya que las variables no fueron manipuladas intencionalmente, sino que se observaron dentro de su entorno natural; es transversal porque la recolección de datos se llevó a cabo en un único punto en el tiempo. Este diseño resulta adecuado para caracterizar la situación actual de un fenómeno y sugerir soluciones estructuradas basadas en evidencia empírica.

Población y Muestra

Los trabajadores del Hospital Nivel II La Caleta de Chimbote que estaban relacionados con la gestión y el uso de los sistemas de información institucionales constituyeron la población. Esta se dividió en cinco categorías: médicos (69), obstetras (25), personal administrativo (49), técnicos en tecnologías de información (20) y otros profesionales relacionados con la asistencia, entre los que se encontraban enfermeras y técnicos en enfermería (307). En total, había 470 empleados. Se eligió, a través de un muestreo no probabilístico por juicio, una muestra de 30 participantes que representaban proporcionalmente las áreas mencionadas, con mayor énfasis en aquellos que interactuaban directamente con los sistemas de información clínicos y administrativos.

Técnicas e instrumentos

Se utilizaron dos métodos principales para recopilar información. La primera fue la encuesta, que se realizó utilizando un cuestionario estructurado de 20 ítems con una escala dicotómica (Sí/No). Este cuestionario se creó tomando como base los dominios de la norma ISO/IEC 27001:2022 e incorporó aspectos como las políticas de seguridad, el manejo organizacional, la gestión de accesos, la protección del medioambiente y física, el control de incidentes y operaciones, el cumplimiento normativo y la continuidad del negocio. La segunda fue la entrevista semiestructurada, destinada a los líderes del departamento de TI y a las autoridades institucionales, con el objetivo de profundizar en los procesos operativos, las carencias en cumplimiento y las competencias establecidas en términos de seguridad de la información. Antes de ser aplicados, ambos instrumentos fueron validados a través del juicio de expertos.

Procedimiento

Se llevó a cabo la recopilación de datos en tres etapas. En la fase inicial, se realizó el diagnóstico institucional a través de la implementación del cuestionario sobre el personal escogido y el examen de los documentos de los informes de incidentes de seguridad del año 2024. En la segunda etapa, se utilizó la estadística descriptiva para procesar los datos. Se determinaron las frecuencias absolutas

y los porcentajes por indicador, que fueron clasificados de acuerdo a los dominios de la norma ISO/IEC 27001 con el fin de detectar brechas en el cumplimiento. En la fase número tres, se elaboró el modelo de buenas prácticas a partir de los resultados del diagnóstico. Esto incluyó la estructuración de las políticas, controles técnicos, protocolos para gestionar riesgos y sistemas de capacitación necesarios para corregir las deficiencias detectadas. examinado. Se utilizó Microsoft Excel (versión 2019 de Microsoft Corporation) para procesar estadísticamente los datos, lo que dio lugar a tablas de frecuencia y gráficos de distribución porcentual para cada uno de los indicadores estudiados.

Método de Análisis de datos

Se utilizaron estadísticas univariadas descriptivas para analizar los datos adquiridos. Se calcularon la frecuencia absoluta y el porcentaje de respuestas positivas y negativas para cada elemento del cuestionario, y se registró el indicador numérico resultante como medida de cumplimiento del control evaluado.

Se compararon los resultados con los límites mínimos establecidos por la norma ISO/IEC 27001 para calcular el grado de madurez institucional en cada área. Debido a la naturaleza descriptivo-propositiva de la investigación y al tamaño de la muestra utilizada, no se llevaron a cabo pruebas de inferencia estadística.

RESULTADOS

Un total de 145 incidentes de seguridad de la información se descubrieron en el Hospital Nivel II La Caleta durante el examen de los archivos institucionales del año 2024. Las infecciones por malware fueron la amenaza más importante, con un 32.4% de los casos (n=50), seguidas de fallos humanos y errores de configuración (24.8%; n=36), pérdida o corrupción de datos (16.5%; n=24), entradas no permitidas (13.7%; n=20) y problemas de disponibilidad (10.3%; n=15). Más de la mitad de los incidentes (57,2%) provienen de amenazas técnicas que se pueden prevenir con controles básicos de seguridad; al mismo tiempo, una parte importante (24,8%) está vinculada a carencias en la capacitación del personal. Respecto a la infraestructura tecnológica, se encontró que el 55,5% de los equipos (100 de 180) tienen fallas técnicas persistentes, ninguno tiene antivirus actualizado, 120 no cuentan con políticas para respaldar automáticamente y 30 utilizan sistemas obsoletos. Además, durante el periodo evaluado, se contabilizaron 35 horas de inactividad en el módulo de laboratorio y 24 horas en el sistema de historias clínicas, lo que resultó en un total de 4,320 interrupciones a los sistemas en el último año.

Se muestran a continuación los resultados del cuestionario administrado a 30 participantes, que fueron procesados a través de porcentajes por dominio y frecuencias absolutas. Se ordenan de menor a mayor cumplimiento (Tabla 1).

TABLA 1.

En el Hospital La Caleta, en 2024, se evaluó el grado de cumplimiento de las medidas de seguridad conforme a los dominios ISO/IEC 27001.

Dominio ISO/IEC 27001	*Indicador evaluado*	*Cumplimiento (%)*	*Nivel*
Continuidad del negocio (A.17)	Simulacros de caída de sistemas	5	Muy bajo – crítico

Gestión de riesgos	Aplicación de metodologías de riesgo	5	Muy bajo – crítico
Políticas de seguridad (A.5)	Existencia de políticas formales	20	Bajo
Monitoreo de operaciones (A.12)	Supervisión de sistemas	70	Intermedio
Seguridad del personal (A.6)	Conocimiento de responsabilidades	80	Intermedio
Gestión de activos (A.8)	Control de inventario tecnológico	80	Intermedio
Mantenimiento de equipos (A.11)	Mantenimiento preventivo programado	87	Medio-alto
Control de accesos físicos (A.9/A.11)	Acceso regulado al Data Center	90	Alto

A partir del diagnóstico previo, se creó un modelo de buenas prácticas compuesto por cuatro elementos interrelacionados:

1. Marco normativo y políticas de seguridad, que establece las políticas documentadas, roles y responsabilidades en concordancia con el Anexo A.5 de la ISO/IEC 27001;
2. Gestión de riesgos, fundamentada en la metodología ISO/IEC 27005, que incluye reconocer, analizar, evaluar y manejar los riesgos sobre activos críticos;
3. Controles operativos y técnicos, que abarca la actualización de antivirus, implementación de respaldos automáticos, segmentación de red y supervisión constante de los sistemas; y
4. Capacitación y cultura organizacional a través de programas estructurados para sensibilizar a todo el personal. El modelo incluye indicadores clave de desempeño (KPIs) y un ciclo de mejora continúa llamado PDCA para asegurar

Para asegurar su sostenibilidad a largo plazo, el modelo incluye un ciclo de mejora continua PDCA y KPIs (indicadores de desempeño clave).

DISCUSIÓN

Los resultados de esta investigación corroboran la hipótesis principal del estudio: cuando no existe un modelo organizado de buenas prácticas, se relaciona con altos niveles críticos de vulnerabilidad en la seguridad hospitalaria. La norma ISO/IEC 27001 requiere que se cumplan todos los dominios para obtener la certificación. Sin embargo, el cumplimiento del 20% en políticas formales de seguridad y el 5% en gestión de riesgos y simulacros de continuidad constituyen grandes brechas con respecto a lo mínimo exigido por dicha norma.

Estos resultados concuerdan con los hallazgos reportados en investigaciones similares hechas en el ámbito latinoamericano. Estudios anteriores realizados en hospitales públicos de Ecuador y Colombia descubrieron patrones similares de incumplimiento en cuanto a la gestión de riesgos y políticas de seguridad, con grados de madurez que varían entre el 15% y el 30% en entidades donde no se ha implementado un SGSI. Esta cifra es congruente con el 20% que este estudio actual encontró para el dominio de las políticas formales. Asimismo, investigaciones realizadas en el sector de la salud de Perú indicaron que la razón

principal de incidentes de seguridad es la falta de controles técnicos básicos, especialmente la falta de actualización del software de protección. Este resultado se repite en el 100% de los equipos sin un antivirus actualizado encontrados en el Hospital La Caleta.

Sin embargo, los resultados varían en ciertas áreas en comparación con las experiencias de implementación de SGSI en hospitales privados más grandes, donde el promedio de cumplimiento del control de accesos físicos es superior al 95%. En este estudio, aunque el acceso al Data Center llegó a un alto nivel (90%), este control funciona de forma aislada y no está incluido en un marco normativo oficial, lo que restringe su efectividad y auditabilidad. Esta es una diferencia que diversos autores han indicado como crucial para distinguir entre un control efectivo y una práctica informal.

El 24,8 % de los incidentes relacionados con factores humanos confirma lo que han indicado investigaciones sobre la cultura organizacional en seguridad de la información en la administración pública: que la capacitación del personal es el tipo de intervención más eficaz para disminuir incidentes evitables. En esta línea, el elemento de sensibilización que se incluye en el modelo sugerido responde directamente a esta evidencia, lo cual lo distingue de iniciativas previas que solo se enfocan en los controles técnicos.

Una restricción del estudio actual es el número de la muestra (n=30), que, aunque resulta representativa para el diseño descriptivo empleado, limita que los resultados se extrapolen a otros hospitales de nivel II sin antes haber sido validados en un contexto similar. Asimismo, el diseño transversal no permite evaluar la evolución temporal de las brechas identificadas ni el impacto de las intervenciones propuestas, aspectos que deberán abordarse en estudios longitudinales posteriores a la implementación del modelo. A pesar de estas restricciones, la aportación del trabajo está en proporcionar un modelo adecuado a las condiciones reales de funcionamiento de los hospitales públicos peruanos de nivel II, lo que lo hace diferente de marcos normativos generales y le permite ser una herramienta práctica e inmediata para instituciones con características similares.

CONCLUSIONES

El diagnóstico del estado de seguridad de la información en el Hospital Nivel II La Caleta de Chimbote reveló un nivel de madurez institucional bajo a intermedio, con un cumplimiento promedio del 55,9% sobre los dominios evaluados de la norma ISO/IEC 27001. Los 145 incidentes de seguridad documentados en 2024, liderados por infecciones de malware (32,4%) y pérdida o corrupción de datos (16,5%), además de las 4.320 interrupciones a los sistemas y periodos de inactividad que alcanzan hasta 35 horas en módulos críticos, evidencian la exposición constante a amenazas que ponen en peligro la continuidad del servicio sanitario y la integridad de los datos clínicos y administrativos relacionados con los pacientes.

El análisis de las brechas por dominios mostró que las áreas con mayores carencias son la gestión de riesgos y la continuidad del negocio, con un cumplimiento del 5% en cada caso, así como la formalización de políticas de seguridad, que solo el 20% de los empleados conoce. Estas cifras demuestran que el hospital no ha puesto en marcha un Sistema de Gestión de Seguridad de

la Información, según la norma ISO/IEC 27001. Asimismo, los controles presentes, como el acceso al Data Center regulado (90%) y el mantenimiento preventivo de equipos (87%), funcionan de forma independiente y sin una validación normativa oficial, lo cual reduce su eficacia, trazabilidad y permanencia a largo plazo.

Ante esta situación, el modelo de buenas prácticas sugerido es una respuesta organizada y adaptada a las condiciones operativas y presupuestarias de los hospitales públicos peruanos de nivel II. El modelo, al incorporar las políticas de seguridad, la gestión del riesgo fundamentada en la norma ISO/IEC 27005, los controles técnicos prioritarios y los programas de formación constante del personal dentro de un marco único, se ocupa a la vez de las dimensiones técnicas, organizacionales y humanas que el diagnóstico detectó como los tres pilares de vulnerabilidad del hospital. La inclusión de indicadores clave de rendimiento y un ciclo de mejora continua (PDCA) asegura que el modelo no sea una intervención aislada, sino un sistema de gestión que se puede auditar y que es sostenible, replicable en instituciones hospitalarias públicas de similares características en la región.

BIBLIOGRAFÍA

Carranza, J., & Gómez, H. (2017). Sistema de gestión de seguridad de la información basado en la norma ISO 27001 para el Hospital Nivel II La Caleta. Tesis de maestría, Universidad Privada San Pedro.

Hernández-Sampieri, R., & Mendoza, C. (2022). Metodología de la investigación: Las rutas cuantitativa, cualitativa y mixta. McGraw-Hill Education.

IBM Security. (2022). X-Force Threat Intelligence Index 2022. https://secure-iss.com/wp-content/uploads/2022/11/X-Force-Threat-Intelligence-Index-2022-Full-Report.pdf

International Organization for Standardization. (2022a). ISO/IEC 27001:2022: Information security, cybersecurity and privacy protection — Information security management systems — Requirements. ISO.

International Organization for Standardization. (2022b). ISO/IEC 27002:2022: Information security, cybersecurity and privacy protection — Information security controls. ISO.

International Organization for Standardization. (2022c). ISO/IEC 27005:2022: Information security, cybersecurity and privacy protection — Guidance on managing information security risks. ISO.

Nicho Gómez, M. N. (2024). Modelo de gestión de riesgos para mejorar la seguridad de la información en los procesos de emergencia en el sector salud pública de la región Lambayeque. Tesis de maestría, Universidad Católica Santo Toribio de Mogrovejo.

Rosero Córdoba, J. E. (2024). Recomendar las mejores prácticas en el sector salud basadas en frameworks de ciberseguridad aplicables a hospitales del sector público en Colombia. Trabajo de especialización, Universidad Nacional Abierta y a Distancia.

Sánchez Marín, R. V. (2024). Implementación de un sistema de gestión de información y eventos de seguridad para la detección de amenazas en una entidad pública del sector salud. Investigación de posgrado, Universidad Nacional Tecnológica de

Lima Sur.

Villegas Rivera, C. A. (2022). Modelo de gestión de riesgos de TI que contribuye en la protección de los activos de información en hospitales de nivel II-1 de la región Amazonas. Tesis de maestría, Universidad Católica Santo Toribio de Mogrovejo.

DERECHOS DE AUTOR

COMO CITAR:

Carranza Lujan, J. L. (2026). Modelo de buenas prácticas para seguridad de información en Hospitales Nivel II. *REDSA Revista Ecuatoriana de Desarrollo Social y Ambiental, 1* (3) 1 - 9. https://doi.org/10.66646/redsa-2026/3zv24c78.