Ciencias y Saberes

ISSN 2960-8430

GESTIÓN DE RIESGOS EN TI SEGÚN ISO 27001:2022 EN UNA UNIDAD EDUCATIVA FISCAL DE ECUADOR

Esel Andrés Olvera Peña
tesolver_88@live.com
ORCID: https://orcid.org/0009-0000-3660-1017
Universidad Internacional Iberoamericana (UNIB/UNINI)

Jon Arambarri
jon.arambarri@uneatlantico.es
ORCID: https://orcid.org/0000-0001-8116-8427
Universidad Europea del Atlántico / Escuela Politécnica Superior

Saúl Domingo Soriano
saul_domingo@funiber.org
ORCID: https://orcid.org/0000-0002-7559-6131
Universidad Europea del Atlántico y FUNIBER

Recibido: 18/03/26
Aceptado: 20/04/26
Publicado: 01/05/26

RESUMEN

La protección de la información en los colegios y unidades educativas fiscales del Ecuador sigue siendo, en la práctica, una deuda pendiente. Este trabajo partió de esa realidad concreta y propuso una respuesta metodológica estructurada: aplicar la norma ISO 27001:2022 para identificar, valorar y tratar los riesgos tecnológicos de una institución educativa de nivel medio ubicada en Quevedo, Ecuador. El estudio adoptó un diseño de investigación-acción con enfoque mixto y empleó tres instrumentos de campo: una ficha de observación del área de TI, una encuesta dirigida al personal docente y administrativo y la revisión sistemática de controles mediante el Anexo A de la norma. Los resultados identificaron seis activos tecnológicos con niveles de riesgo medio y alto; entre ellos: cámaras de vigilancia, almacenamiento en red, estaciones de trabajo y puntos de acceso inalámbrico, con puntajes que alcanzan hasta 18 sobre 27 en la escala de riesgo aplicada. Para cada uno de estos activos se elaboraron políticas de seguridad con objetivos claros, acciones operativas específicas e indicadores verificables, adaptadas a las condiciones reales de la institución.

Palabras clave: ISO 27001:2022, gestión de riesgos TI, seguridad de la información, institución educativa pública.

IT RISK MANAGEMENT BASED ON ISO 27001:2022 IN AN ECUADORIAN PUBLIC SCHOOL

ABSTRACT

Information security in Ecuador's public schools and educational institutions remains, in practice, an unresolved issue. This study began with this specific reality and proposed a structured methodological approach: applying the ISO 27001:2022 standard to identify, assess, and address the technological risks of a secondary school located in Quevedo, Ecuador. The study adopted a mixed-methods action research design and employed three field instruments: an IT observation checklist, a survey of teaching and administrative staff, and a systematic review of controls using Annex A of the standard. The results identified six technological assets with medium and high-risk levels, including surveillance cameras, network storage, workstations, and wireless access points, with scores reaching up to 18 out of 27 on the applied risk scale. For each of these assets, security policies were developed with clear objectives, specific operational actions, and verifiable indicators, adapted to the institution's actual conditions.

Key words: ISO 27001:2022, IT risk management, information security, public school.

Correo principal para contacto: tesolver_88@live.com

1. INTRODUCCIÓN

Cuando se habla de la información en el sector educativo público de Ecuador, todavía suena, en muchos contextos, como algo lejano o de menor prioridad frente a las urgencias cotidianas del aula. Sin embargo, quienes trabajan directamente en esas instituciones conocen bien la otra cara de esa percepción: docentes que registran calificaciones sin ningún tipo de protección, laboratorios conectados a servidores ministeriales con credenciales débiles y responsables de TI que atienden en solitario a cientos de usuarios. Este contraste, entre la magnitud real del riesgo y la escasez de controles existentes, constituye, precisamente, el punto de partida de este estudio.

La digitalización llegó a las aulas, sí, pero no llegó de manera uniforme. El Ministerio de Educación dispone hoy de plataformas en línea para registros de calificaciones, planificaciones curriculares y gestión administrativa; mientras tanto, las unidades educativas fiscales siguen sin la infraestructura ni la cultura organizacional necesarias para proteger esos mismos procesos. La Ley Orgánica de Educación Intercultural (LOEI) y la Ley Orgánica de Protección de Datos Personales (LOPD) establecen obligaciones claras al respecto, pero su cumplimiento en instituciones públicas sigue siendo parcial (Ruiz Tapia et al., 2020). A esto, se suma una tendencia global documentada: el sector educativo se ha convertido en blanco frecuente de ciberataques, especialmente desde la aceleración del uso de plataformas digitales (Andrade Vintimilla, 2023).

Frente a ese panorama, la norma ISO 27001 ofrece un camino reconocido y probado. Su versión 2022 reorganizó el catálogo de controles del Anexo A en cuatro bloques temáticos: organizacionales, de personas, físicos y tecnológicos, reduciendo el total de 114 a 93 controles con mayor coherencia práctica (ISO, 2022). Al mismo tiempo, el Ministerio de Telecomunicaciones del Ecuador dispone de una guía propia para la gestión de riesgos en el sector público que resulta compatible con la lógica de la norma y facilita su adopción en contextos institucionales como el de las unidades educativas fiscales (MINTEL, 2020).

A partir de ese diagnóstico, este estudio se propuso identificar los activos tecnológicos más vulnerables de una escuela de Quevedo, Ecuador, calcular su nivel de riesgo con datos reales recogidos en campo y formular políticas de seguridad que la institución pueda adoptar de forma progresiva.

2. ESTRATEGIAS METODOLÓGICAS / MATERIALES Y MÉTODOS

El estudio combinó un enfoque cualitativo y cuantitativo, bajo un diseño de investigación-acción (Hernández Sampieri et al., 2016). El componente cualitativo permitió comprender cómo el personal percibe y gestiona la seguridad en su quehacer cotidiano, mientras que el componente cuantitativo calcula con precisión el nivel de riesgo de cada activo tecnológico. La articulación de ambos enfoques facilita tanto el diagnóstico de la situación como el diseño de respuestas concretas y contextualmente pertinentes.

La institución seleccionada es una unidad educativa fiscal de jornada matutina con modalidad presencial, ubicada en el sector urbano del cantón Quevedo, provincia

de Los Ríos. Esta atiende a 1.515 estudiantes, distribuidos desde Básica Superior hasta Bachillerato Técnico en tres especialidades: Electricidad, Mecánica Automotriz y Construcciones Metálicas. Su planta docente está conformada por 63 profesionales.

Toda la operación tecnológica de la institución red interna, computadores del personal, laboratorio de informática y conectividad con el sistema de gestión del Ministerio de Educación depende de un único encargado de TI. Este sistema ministerial reside en un servidor en la nube de propiedad del Ministerio y puede accederse desde tres puntos: los equipos administrativos de la institución, los computadores del laboratorio y los dispositivos personales que docentes y estudiantes utilizan desde sus hogares.

Participantes e instrumentos de recolección de información. Participaron en la investigación los 63 docentes de la institución, el personal administrativo y el encargado del área de TI. Todos ellos tienen contacto directo con la información institucional en alguna de sus formas. En este sentido, se utilizaron tres instrumentos complementarios:

- Una ficha de observación con ocho indicadores, aplicada directamente en el área de TI, para levantar el estado real de los equipos, la infraestructura de red y las prácticas de mantenimiento existentes.

- Una encuesta de diez preguntas cerradas dirigida al personal docente y administrativo, orientada a medir los hábitos de seguridad digital y el nivel de conocimiento sobre las políticas institucionales vigentes.

- La revisión del Anexo A de la norma ISO 27001:2022, adaptada al contexto específico de la institución, para determinar qué controles existen, cuáles están en proceso de implementación y cuáles no han sido aplicados.

Cálculo del nivel de riesgo. Para estimar el nivel de riesgo de cada activo se siguió la metodología propuesta por el MINTEL (2020), que valora los activos a partir de tres dimensiones clásicas: Confidencialidad (C), Integridad (I) y Disponibilidad (D). A partir de esas tres puntuaciones se obtiene el Valor del Activo (VA) mediante un promedio simple:

$$\textbf{(1)}\ VA = (C + I + D) / 3$$

Este valor se cruza luego con la probabilidad que ocurra una amenaza y con el grado de exposición del activo ante ella:

$$\textbf{(2)}\ \text{Nivel de riesgo} = VA \times \text{Nivel de amenaza} \times \text{Nivel de vulnerabilidad}$$

Las escalas numéricas que sustentan estas fórmulas se detallan en las Tablas 1, 2 y 3. En todos los casos, valores entre 1 y 3 se consideran riesgos tolerables; a partir de 4, se requiere algún tipo de intervención.

Tabla 1

Valoración del impacto en las dimensiones CID.

Dimensión	Crítico (3)	Mayor (2)	Moderado (1)	Menor (0)
Confidencialidad	Datos altamente sensibles.	Acceso restringido.	Uso interno.	Información pública.
Integridad	Daño grave a los datos.	Afectación moderada.	Alteración leve.	Sin consecuencias.
Disponibilidad	Paralización crítica de operaciones.	Afectación notable.	Impacto leve.	Impacto casi nulo.

Nota. Guía para la gestión de riesgos de seguridad de la información. *Fuente:* autoría propia, adaptada de MINTEL (2020).

Tabla 2

Escalas de probabilidad de amenazas y vulnerabilidades.

Nivel	Valor	Criterio de amenaza	Criterio de vulnerabilidad
Alto	3	Muy probable (>50%).	Ninguna medida de seguridad instalada.
Medio	2	Probable por descuidos o errores.	Las medidas existentes no son suficientes.
Bajo	1	Poco probable (<50%).	La medida implementada es efectiva.

Nota. Guía para la gestión de riesgos de seguridad de la información. *Fuente:* autoría propia, adaptada de MINTEL (2020).

Tabla 3

Umbrales para clasificar el nivel de riesgo.

Nivel de riesgo	Puntaje obtenido
Alto	9 a 27
Medio	4 a 8
Bajo	1 a 3

Nota. Guía para la gestión de riesgos de seguridad de la información. *Fuente:* autoría propia, adaptada de MINTEL (2020).

Fases del trabajo. El estudio se desarrolló en tres etapas que se retroalimentaron mutuamente a lo largo del proceso:

- Diagnóstico situacional: el trabajo comenzó con la recolección de información mediante los tres instrumentos descritos anteriormente, con el propósito de trazar un

mapa claro del estado actual de la seguridad en la institución. Esta fase fue imprescindible para que las etapas siguientes partieran desde evidencia concreta y no de supuestos.

- Valoración de riesgos: con el diagnóstico en mano, se identificaron y priorizaron los activos más comprometidos, aplicando las fórmulas (1) y (2) para cuantificar el nivel de riesgo de cada uno de forma objetiva y reproducible. El uso de una escala numérica fue clave para poder ordenar las prioridades de intervención.

- Diseño de respuestas: para los activos con riesgo medio y alto se redactaron políticas de seguridad contextualizadas, cada una con un objetivo específico, acciones concretas a implementar e indicadores medibles que permiten verificar su cumplimiento en el tiempo.

3. RESULTADOS

La visita al área de TI y las instalaciones de la institución dejó una imagen que muchos docentes conocen bien, aunque no siempre puedan nombrarla con precisión: hay equipos que funcionan, pero nadie lleva un registro de cuándo recibieron mantenimiento por última vez. Las cámaras de seguridad graban, los sensores de movimiento están activos y el firewall opera, pero ninguno de esos dispositivos cuenta con bitácoras de revisión ni protocolos escritos de operación.

Cuatro hallazgos merecen atención especial. Primero, las puertas de oficinas y laboratorios siguen abriéndose con llaves convencionales, a pesar que hay alarmas instaladas en otras partes del edificio, lo que genera una incoherencia que deja flancos abiertos. Segundo, cuando ocurre algún problema de seguridad en la red, quien interviene no es el encargado de TI del plantel, sino técnicos del proveedor de internet (Corporación Nacional de Telecomunicaciones) o del Distrito de Educación, lo que implica tiempos de respuesta prolongados e información sensible que pasa por manos externas sin un protocolo formal de confidencialidad. Tercero, no existe ningún registro documentado de incidentes pasados, lo que impide aprender de los errores. Cuarto, no hay un inventario oficial de los activos tecnológicos ni políticas escritas que regulen su uso.

Posteriormente, se aplicó la encuesta a 63 docentes y al personal administrativo. La Tabla 4 sintetiza las respuestas en los aspectos más relevantes para este estudio.

Tabla 4

Hábitos y conocimientos de seguridad digital del personal.

Pregunta formulada	Sí / Siempre	No / Nunca
¿Usa contraseña o PIN en su laptop personal?	35%	65%
¿Actualiza regularmente su sistema operativo?	22%	78%
¿Se conecta a la red institucional de forma segura?	48%	52%
¿Tiene cuidado al abrir correos y archivos adjuntos?	100%	0%

¿Respalda su información con regularidad?	16%	84%
¿Conoce las políticas de contraseñas de la institución?	0%	100%
¿Reporta los incidentes de seguridad que detecta?	100%	0%
¿Ha recibido capacitación en seguridad de la información?	0%	100%
¿Considera necesario que la institución tenga políticas de seguridad?	100%	0%

Nota. Encuesta aplicada al personal docente y administrativo de la Unidad Educativa.
Fuente: autoría propia.

En este contexto, los datos revelan una paradoja que merece ser subrayada: el 100% del personal considera que la institución debe contar con políticas de seguridad, y ese mismo porcentaje afirma reportar los incidentes cuando los detecta. Sin embargo, también el 100% afirma no conocer ninguna política institucional y no haber recibido capacitación alguna en seguridad de la información. En la práctica cotidiana, el 84% no realiza respaldos de sus datos y el 78% trabaja con sistemas operativos desactualizados. El diagnóstico que emerge de esos números no apunta a falta de voluntad, sino a ausencia de estructura: la disposición existe, pero falta arquitectura organizacional que la encauce.

Finalmente, la revisión del Anexo A arrojó el panorama que se detalla en la Tabla 5. Conviene aclarar que el 48% catalogado como 'no aplica' corresponde a controles diseñados para organizaciones de mayor complejidad como hospitales o entidades financieras que no resultan pertinentes para una unidad educativa de estas características.

Tabla 5

Nivel de cumplimiento de los controles del Anexo A, ISO 27001:2022.

Nivel de madurez	Descripción	% de controles
No aplica	Control no pertinente al contexto institucional.	48%
Inexistente	No hay política, procedimiento ni control alguno.	15%
Optimizado	Funciona correctamente y se monitorea de forma continua.	13%
Limitado	En desarrollo, aún incompleto.	11%
Gestionado	Implementado recientemente y en operación.	8%
Definido	Casi terminado, pero sin implementación total.	5%
Inicial / sin revisar	No ha sido evaluado todavía,	0%
	Total	**100%**

Fuente: autoría propia adaptado del Anexo A de la norma ISO 27001:2022.

Del 52% restante de los controles efectivamente aplicables a la institución, un preocupante 15% no existe en ninguna forma. Las áreas con mayor desprotección son: gestión de vulnerabilidades técnicas, prevención de fuga de datos, copias de seguridad, segmentación de redes, cifrado y seguridad en aplicaciones web. En conjunto, esas ausencias dejan a la institución expuesta a prácticamente cualquier tipo de ataque dirigido o incluso a incidentes no intencionales de considerable impacto.

Mapa de riesgos por activo. Con base en la información recogida se construyó un mapa de riesgos para los activos tecnológicos de la institución. La Tabla 6 presenta la categorización inicial de los activos a nivel de infraestructura de TI, con los riesgos asociados identificados durante el diagnóstico.

Tabla 6

Activos tecnológicos y riesgos asociados en la infraestructura de la institución.

Activo	Principal riesgo detectado	Tipo de afectación
Servidor	Fallo de redundancia en el servidor central.	Disponibilidad.
Switch	Manipulación de configuración por ingeniería social.	Integridad / seguridad de red.
NAS (almacenamiento en red)	Acceso no autorizado a datos almacenados.	Confidencialidad / integridad.
Estaciones de trabajo docentes	Pérdida de datos por ausencia de copias de seguridad.	Integridad / confidencialidad.
Puntos de acceso Wi-Fi	Acceso externo no autorizado a la red inalámbrica.	Seguridad de red / confidencialidad.
Firewall	Configuración deficiente que admite tráfico no deseado.	Seguridad de red.
Servidor de correo	Ataques de denegación de servicio (DoS).	Disponibilidad.
Software antivirus	Firmas desactualizadas que reducen la capacidad de detección.	Integridad / seguridad del sistema.

Fuente: autoría propia.

Aplicando las ecuaciones (1) y (2) sobre los seis activos que acumularon más factores de riesgo durante el diagnóstico, se obtuvieron los resultados que muestra la Tabla 7: cuatro de ellos superaron el umbral correspondiente a riesgo alto (puntaje ≥ 9), mientras que dos quedaron en la categoría media.

Tabla 7

Nivel de riesgo calculado para los seis activos más vulnerables.

Activo	C	I	D	VA	Amenaza	Vuln.	Resultado
Cámaras de seguridad.	2	2	2	2	3	3	18 alto
Sensores de movimiento.	1	2	3	2	2	3	12 alto
NAS	3	3	3	3	2	3	18 alto
Estaciones de trabajo docentes.	2	3	2	2	3	2	12 alto
Puntos de acceso Wi-Fi.	2	2	2	2	2	2	8 medio
Antivirus	1	2	3	2	2	2	8 medio

Nota. C = Confidencialidad, I = Integridad, D = Disponibilidad, VA = Valor del Activo, Vuln. = Vulnerabilidad. *Fuente:* autoría propia.

El almacenamiento en red (NAS) y las cámaras de seguridad encabezan la lista con un puntaje de 18, lo que los convierte en prioridad absoluta de intervención. El primero concentra datos sensibles, sin ningún tipo de cifrado y con controles de acceso inexistentes; las cámaras, por su parte, operan sin contraseñas robustas y con transmisiones sin cifrar, lo que las expone tanto a ataques externos como a manipulaciones internas de consecuencias difíciles de prever.

Políticas de seguridad propuestas. Para cada uno de los seis activos críticos identificados se diseñó una política de seguridad. La Tabla 8 ofrece una visión de conjunto; a continuación, se desarrollan los aspectos más relevantes de cada una.

Tabla 8

Síntesis de las políticas propuestas para los activos con riesgo medio y alto.

Activo	Medidas centrales	Indicador de verificación
Cámaras de seguridad.	Mantenimiento programado con bitácora, protección física, contraseñas de mínimo 12 caracteres renovadas cada 90 días, monitoreo activo con registro de accesos.	Registro mensual de revisiones y accesos.
Sensores de movimiento.	Cifrado de comunicaciones con TLS 1.2 o superior; autenticación por certificado digital por dispositivo; auditoría semestral de configuraciones.	Informe semestral de auditoría de configuraciones.
NAS	Acceso por roles (RBAC) con principio de mínimo privilegio; cifrado en reposo con BitLocker o equivalente; registro mensual de accesos revisado por TI y reportado a Dirección.	Informe mensual de actividad en el NAS.

Estaciones de trabajo docentes.	Antivirus con actualizaciones diarias; parches de seguridad aplicados dentro de 15 días tras su lanzamiento; contraseñas con rotación bimestral; control de acceso físico fuera del horario.	Auditoría trimestral del estado de los equipos.
Puntos de acceso Wi-Fi.	WPA3 o WPA2-Enterprise; tres VLANs independientes (administración, docentes, estudiantes); protección ante ataques DoS; actualización de firmware cada trimestre.	Escaneo mensual de la red inalámbrica.
Antivirus.	Actualizaciones automáticas diarias de firmas; actualización mensual del motor central; ajuste fino de reglas para reducir falsos positivos; protocolo documentado de cuarentena y reporte.	Reporte semanal del estado del software.

Nota. RBAC = Role-Based Access Control. Fuente: autoría propia.

Cámaras de seguridad y sensores de movimiento. Estos dispositivos requieren, como condición de base, un programa formal de mantenimiento: fechas establecidas, responsables identificados y un registro escrito de cada intervención. El sistema de vigilancia no puede seguir operando sin esa trazabilidad mínima. En cuanto a las credenciales de acceso, es indispensable que sean complejas: al menos 12 caracteres combinando letras, números y símbolos y que se renueven cada 90 días sin excepción. Para los sensores, la prioridad es cifrar todas las comunicaciones con el sistema central mediante TLS 1.2 o superior e incorporar autenticación por certificado digital, para que ningún dispositivo no autorizado pueda integrarse a la red de vigilancia.

Almacenamiento en red (NAS). El NAS guarda información que, en manos equivocadas, podría comprometer a toda la comunidad educativa: datos de estudiantes, registros administrativos y documentación interna de carácter sensible. Por esa razón, el acceso tiene que quedar restringido al personal que lo necesita para cumplir su función específica, aplicando el principio de mínimo privilegio a través de un sistema de control de acceso basado en roles (RBAC). Todo lo que se almacene en este dispositivo debe cifrarse en reposo con BitLocker o una solución técnicamente equivalente. Complementariamente, se propone generar un registro mensual de accesos que sea revisado por el encargado de TI y reportado a la dirección institucional cada vez que se detecte alguna actividad inusual.

Estaciones de trabajo de los docentes. La combinación de sistemas operativos desactualizados y ausencia de respaldos regulares es, quizás, el escenario de mayor riesgo cotidiano para la información docente. La política propuesta establece que los parches de seguridad deben aplicarse dentro de los 15 días siguientes a su lanzamiento, que el antivirus se actualice automáticamente cada día y que las contraseñas de inicio de sesión se renueven cada dos meses. Se contempla también restringir el acceso físico a los equipos fuera del horario laboral. Para verificar el cumplimiento, el encargado de TI realizará auditorías trimestrales con reporte formal a la dirección.

Puntos de acceso Wi-Fi. Una red inalámbrica sin segmentación es un entorno donde cualquier dispositivo conectado puede, en principio, acceder a los mismos recursos que cualquier otro. Para corregir esa situación, la propuesta contempla dividir

la red en tres segmentos independientes: uno para el área administrativa, otro para los docentes y otro para los estudiantes, con controles de acceso diferenciados en cada caso. Adicionalmente, se requiere configurar mecanismos de detección y bloqueo automático de ataques de denegación de servicio (DoS), actualizar el firmware de los puntos de acceso cada trimestre y migrar a WPA3 o, como mínimo, a WPA2-Enterprise.

Software antivirus. Un antivirus con firmas desactualizadas deja de ser una defensa efectiva para convertirse en una falsa sensación de seguridad. La política establece que las actualizaciones de firmas se descarguen automáticamente cada día y que el motor central se actualice cada mes. Es igualmente importante depurar las reglas de detección para reducir los falsos positivos, que generan fatiga en el personal y terminan siendo ignorados. Ante la detección de un archivo sospechoso, el protocolo de respuesta indicado es el siguiente: cuarentena inmediata, notificación al encargado de TI, análisis del incidente y comunicación a la dirección si existe riesgo de que los datos institucionales estén comprometidos.

4. DISCUSIÓN

Los resultados de este estudio difícilmente sorprenden a quienes conocen de cerca las dinámicas de las instituciones educativas fiscales en Ecuador. La brecha entre lo que la normativa exige y lo que los centros escolares pueden hacer con sus presupuestos y su dotación de personal es estructuralmente amplia. Pero cuando los datos se expresan en números, esa brecha resulta difícil de ignorar: activos con puntajes de riesgo que superan los dos tercios del máximo posible y un personal sin una sola jornada de formación en seguridad digital. Esta combinación no es simplemente preocupante desde el punto de vista técnico, es una vulnerabilidad latente que, en cualquier momento, puede materializarse en consecuencias serias para estudiantes, docentes e institución.

Investigaciones previas realizadas en contextos similares llegaron a conclusiones análogas. Amaya Díaz (2022) documentó en Colombia un cuadro prácticamente idéntico al observado en este estudio; Lara Guachamin (2023) describió una situación comparable en otra unidad educativa de Guayaquil y Andrade Vintimilla (2023) advirtió que la pandemia de COVID-19 aceleró la exposición digital de los centros educativos sin que se adoptaran las medidas de protección correspondientes. Lo que distingue al presente trabajo de esos antecedentes es el uso simultáneo del Anexo A de la versión más actualizada de la norma la de 2022, más coherente y práctica que la de 2013 y de la metodología cuantitativa del MINTEL, que produce un cálculo de riesgos más alineado con la realidad operativa del sector público ecuatoriano.

El contraste que reveló la encuesta: el 100% del personal quiere políticas, pero el 100% no conoce ninguna, no apunta a un problema de actitud sino de gestión institucional. El personal está dispuesto, lo que falta es que la organización tome decisiones y las comunique de forma sistemática. Este hallazgo coincide con lo señalado por Estrada-Esponda et al. (2021), quienes demostraron que la capacitación continua es el factor que más incide en la efectividad real de cualquier estrategia de seguridad de la información. Dos jornadas formativas anuales, bien planificadas y orientadas a la realidad del centro, podrían modificar ese escenario de manera significativa sin requerir una inversión presupuestal elevada.

La elección metodológica de combinar ISO 27001:2022 con la guía MINTEL también amerita una justificación explícita. La norma internacional aporta el lenguaje, la estructura y el marco de controles que permiten la comparación con otras organizaciones y abren la puerta a una eventual certificación. La guía del MINTEL, por su parte, traduce ese lenguaje al contexto del sector público ecuatoriano y ofrece criterios cuantitativos más manejables para un encargado de TI sin formación especializada en seguridad de la información. Crespo-Martínez y Cordero-Torres (2019) ya señalaban que ninguna metodología es universalmente superior: su pertinencia depende del contexto de aplicación. En este caso particular, la combinación resultó adecuada y replicable en instituciones de características similares.

Una limitación importante que conviene reconocer es que todo lo propuesto tiene, por ahora, carácter de recomendación. Al tratarse de una institución fiscal, cualquier modificación real en sus procedimientos requiere pasar por el Distrito de Educación, lo que puede extender considerablemente los tiempos de implementación. Esto no invalida el trabajo ni reduce su valor como ejercicio metodológico, pero sí obliga a ser precisos sobre su alcance actual y sobre las condiciones necesarias para que las políticas diseñadas se conviertan en práctica efectiva. Una segunda limitación tiene que ver con el alcance del análisis cuantitativo: activos como el servidor de correo, el switch y el firewall identificados en la Tabla 6 como parte del inventario institucional no fueron incluidos en el cálculo de riesgo de la Tabla 7 porque, durante el diagnóstico, se constató que su nivel de exposición resultaba inferior al de los seis activos priorizados. Su seguimiento queda pendiente para una segunda fase de auditoría.

5. CONCLUSIONES / CONSIDERACIONES FINALES

La unidad educativa estudiada opera en una situación de vulnerabilidad que, lejos de ser excepcional, refleja el estado habitual de buena parte de los colegios fiscales del Ecuador. No existen auditorías de seguridad, no hay políticas escritas, no se capacita al personal y no hay un inventario formal de los activos tecnológicos. El hecho que el plantel funcione sin incidentes graves hasta el momento no significa que el riesgo no exista, significa, más bien, que todavía no se ha materializado.

Consecuentemente, la revisión del Anexo A de ISO 27001:2022 confirmó que el 15% de los controles aplicables al contexto institucional, simplemente, no existe en ninguna forma, mientras que apenas el 13% se encuentra en un estado que puede considerarse satisfactorio. Esa asimetría no se resuelve de manera espontánea: requiere decisiones institucionales, asignación de recursos y tiempo. El plan de implementación progresiva propuesto en este estudio intenta ser realista al respecto, priorizando los seis activos que concentran los mayores niveles de riesgo.

De esta manera, el NAS y las cámaras de seguridad emergieron como los activos más críticos, con puntajes de riesgo de 18 sobre 27, seguidos por las estaciones de trabajo de los docentes y los sensores de movimiento, ambos con 12. Para cada uno de estos activos se diseñaron políticas con objetivos claros, acciones operativas precisas e indicadores de verificación que permiten comprobar si se están cumpliendo. La existencia de esos indicadores es, quizás, uno de los aportes más prácticos de este trabajo, porque convierte las recomendaciones en compromisos evaluables.

Adicional, la investigación demostró que la combinación de ISO 27001:2022 y la guía del MINTEL demostró ser un enfoque viable y pertinente para instituciones públicas ecuatorianas con recursos limitados. Por ello, se recomienda al Ministerio de Educación explorar su adopción como estándar para las auditorías periódicas de seguridad en unidades educativas fiscales a escala nacional.

Finalmente, para dar continuidad a este trabajo, se propone: ejecutar una prueba piloto con las seis políticas diseñadas durante al menos seis meses; simular ataques controlados antes de la implementación definitiva para medir la efectividad real de los controles; extender la metodología a otras instituciones del cantón Quevedo y de la provincia de Los Ríos y diseñar un programa de formación en seguridad digital estructurado y sostenible para el conjunto del sector educativo público.

6. REFERENCIAS

Amaya Díaz, H. F. (2022). *Diseño de un SGSI basado en la ISO/IEC 27001 para el liceo Moderno José Celestino Mutis de San Sebastián de Mariquita* [Tesis de Maestría, Universidad Nacional Abierta y a Distancia - UNAD]. https://repository.unad.edu.co/handle/10596/48382

Andrade Vintimilla, J. F. (2023). Plan de ciberseguridad para la educación básica ecuatoriana contra el ciberdelito por COVID-19. *INNDEV - Innovation & Development Ciencias del Sur*, *2*(1), 34. https://www.itscs-cicc.com/ojs/index.php/inndev/article/view/52

Crespo-Martínez, E., y Cordero-Torres, G. (2019). Estudio comparativo entre las metodologías CRAMM y MAGERIT para la gestión de riesgo de TI en las Mipymes. *UDA AKADEM*, (1), 38-47. https://doi.org/10.33324/udaakadem.vi1.129

Estrada-Esponda, R. D., Unás-Gómez, J. L., y Flórez-Rincón, O. E. (2021*).* Prácticas de seguridad de la información en tiempos de pandemia. Caso Universidad del Valle, sede Tuluá. *Revista Logos Ciencia & Tecnología*, *13*(3), 98-110. https://doi.org/10.22335/rlct.v13i3.1446

Hernández Sampieri, R., Fernández Collado, C., y Baptista Lucio, P. (2016). *Metodología de la investigación* (6.ª ed.). McGraw-Hill

Lara Guachamin, T. J. (2023). *Implementación de un SGSI basado en la norma ISO 27001 en la unidad educativa "El Libertador"* [Tesis, Universidad de Guayaquil]. http://repositorio.ug.edu.ec/handle/redug/67415

Ministerio de Telecomunicaciones y de la Sociedad de la Información del Ecuador [MINTEL]. (2020). *Guía para la gestión de riesgos de seguridad de la información.* Subsecretaría de Estado - Gobierno Electrónico. https://www.gobiernoelectronico.gob.ec/wp-content/uploads/2020/04/GUIA-PARA-LA-GESTION-DE-RIESGOS-DE-SEGURIDAD-DE-LA-INFORMACION-ABRIL-2020.pdf

International Organization for Standardization. (2022). *ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection — Information security management systems — Requirements*. https://www.iso.org/standard/27001

Ruiz Tapia, J. A., Estrada Gutiérrez, C. E., y Sánchez Paz, M. (2020). Propuesta de un modelo de un sistema de gestión de calidad en seguridad de la información basado en la norma ISO 27001 para instituciones educativas. *Latinoamericana en Competitividad Organizacional RILCO*, *2*(5), 10. https://www.eumed.net/rev/rilco/05/gestion-instituciones.html