DOI: https://doi.org/10.46296/ig.v9i17.0338

PROTECCIÓN DE DATOS Y NORMATIVAS PARA AUDITORÍAS INFORMÁTICAS

DATA PROTECTION AND REGULATIONS FOR IT AUDITS

Almeida-Zambrano Edison Ernesto [1]; Vélez-Manzaba Diana Gema [2];
Zambrano-Pilay Enrique Cristóbal [3]; Asencio-Domínguez Álvaro Jesús [4]

[1] Universidad Laica Eloy Alfaro de Manabí. Manta, Ecuador.
Correo: edison.almeida@uleam.edu.ec. ORCID ID: https://orcid.org/0000-0002-1601-3450.

[2] Escuela Superior Politécnica Agropecuaria de Manabí Manuel Félix López. Calceta, Ecuador.
Correo: dgvelez@espam.edu.ec. ORCID ID: https://orcid.org/0009-0009-5544-4171.

[3] Universidad De Cádiz. Cádiz, España.
Correo: enrique.zambranopilay@alum.uca.es. ORCID ID: https://orcid.org/0000-0002-9329-0929.

[4] Universidad Estatal del Sur de Manabí. Jipijapa, Ecuador.
Correo: asencio-alvaro7491@unesum.edu.ec.

Resumen

La protección de los datos de carácter personal y la auditoría informática son las bases sobre las que se erige la gestión de la seguridad de la información en la actualidad. Este trabajo estudia tanto el contexto normativo como el contexto técnico en el que se desarrolla la protección de datos y la relación que existe con la auditoría informática, ya que estudia a partir de estándares internacionales y de la normativa ecuatoriana. Por medio de una revisión teórica se analizan las principales herramientas, como son la Ley Orgánica de Protección de Datos Personales, la norma ISO/IEC 27001 y la norma del Reglamento General de Protección de Datos (GDPR por sus siglas en inglés). Los resultados muestran que la auditoría informática permite evaluar el cumplimiento, detectar riscos y nutrir los controles de seguridad de los sistemas de información. La auditoría informática, además, suma la inclusión de estándares internacionales con las normas locales, lo que hace que se mejore la gestión de los datos y la protección de la información, aunque en este sentido también surgen retos relacionados con la implementación, la formación o la adaptación organizacional. La auditoría informática, al igual que un marco normativo robusto, concluye siendo una necesidad si se quiere apostar por garantizar la seguridad de la información y el cumplimiento legal en los entornos digitales.

Palabras clave: protección de datos, auditoría informática, seguridad de la información, ISO 27001, normativa.

Abstract

The protection of personal data and IT auditing are the foundations upon which information security management is currently built. This paper studies both the regulatory and technical context in which data protection develops and its relationship with IT auditing, as it examines the topic based on international standards and Ecuadorian regulations. Through a theoretical review, the main tools are analyzed, such as the Organic Law on the Protection of Personal Data, the ISO/IEC 27001 standard, and the General Data Protection Regulation (GDPR). The results show that IT auditing allows for the evaluation of compliance, the detection of risks, and the strengthening of information systems security controls. IT auditing also incorporates international standards alongside local regulations, improving data management and information protection. However, this also presents challenges related to implementation, training, and organizational adaptation. Like a robust regulatory framework, IT auditing is ultimately essential for ensuring information security and legal compliance in digital environments.

Información del manuscrito:
Fecha de recepción: 09 de enero de 2026.
Fecha de aceptación: 10 de marzo de 2026.
Fecha de publicación: 17 de abril de 2026.

Keywords: data protection, IT auditing, information security, ISO 27001, regulations.

1. Introducción

En el contexto digital actual la protección de los datos de carácter personal está siendo un aspecto esencial para garantizar la seguridad de la información y la generadora de confianza en los sistemas tecnológicos, y que supone una expansión de la base teórica que dio paso a la elaboración de marcos normativos que fuesen necesarios para regular el tratamiento de datos y los derechos de los usuarios (Sampieri, D. et al. 2023). Es en este sentido que la auditoría informática puede considerarse como una herramienta esencial para verificar el cumplimiento de aquéllos y para verificar la integridad de los sistemas de información. A nivel internacional, la norma ISO/IEC 27001 ha generado pautas sobre la gestión de la seguridad de la información en la que dar importancia al enfoque basado en riesgos (ISO, 2022), que permite identificar las vulnerabilidades y dar paso a controles adecuados. Además de ello, a norma ISO/IEC 27701 (ISO, 2023) es complementaria y genera un paso más allá porque nos habla de la gestión de la privacidad de los datos considerando también principios de protección de la información personal.

Por otro lado, en el ámbito ecuatoriano la Ley Orgánica de Protección de Datos Personales (Asamblea Nacional del Ecuador, 2021) fue un paso importante y significativo para regular el tratamiento de los datos al establecer obligaciones para las organizaciones y derechos para los ciudadanos. La Superintendencia de Protección de Datos Personales (2025) ha generado guías técnicas de gestión de riesgos y elaboración de las evaluaciones de impacto sobre el tratamiento de los datos. Como conclusión, este artículo tiene como propósito introducir la protección de datos y las normativas que son aplicables en la auditoría informática considerando tres ejes principales: El concepto de protección de datos, el de auditoría informática y el de los obstáculos para su consolidación.

2. Fundamentos de la protección de datos y seguridad de la información

La protección de datos personales está fundamentada en principios que pretenden asegurar la privacidad, la confidencialidad y el uso adecuado de la información. En este sentido, la normativa internacional ha creado estándares que nos permiten poder establecer sistemas de gestión de la seguridad de la información. La norma ISO/IEC 27001, por su parte, define un conjunto de requerimientos para implementar un sistema de gestión de la seguridad de la información, mediante el análisis de riesgos (ISO, 2022). Este sistema nos va a permitir poder identificar las amenazas, evaluar las vulnerabilidades y establecer controles para mitigar los riesgos; así mismo, la norma ISO/IEC 27701 expande este sistema de gestión de la seguridad de la información mediante la gestión de la privacidad, proveyendo directrices para el tratamiento de datos (ISO, 2023).

Por otro lado, el Reglamento General de Protección de Datos (GDPR) ha establecido principios como la minimización de datos, la transparencia y la responsabilidad en el tratamiento de la información (Hjerppe et al., 2019), principios que han modificado las legislaciones de varios países, incluido Ecuador.

En el plano nacional, la Ley Orgánica de Protección de Datos Personales establece los derechos de los propietarios de los datos como los derechos de las organizaciones, aun cuando la ley prioriza un enfoque en la protección de la privacidad (Asamblea Nacional del Ecuador, 2021).

Además, estudios recientes han planteado que es necesaria la integración de los modelos de gestión de riesgos y su aplicación para el cumplimiento legislativo, yendo por un camino que esté basado en estándares internacionales (Flores & Perugachi, 2023).

Las bases de la protección de datos personales no son más que la integración de normativas y estándares para la seguridad de la información y la privacidad de los usuarios.

3. Auditoría informática y cumplimiento normativo

La auditoría informática es un proceso que se lleva a cabo de forma sistemática durante el cual se evalúan la seguridad, la eficiencia y el cumplimiento de los sistemas de información, cuya finalidad principal consiste en identificar riesgos, auditar controles y verificar el cumplimiento normativo de las organizaciones. La auditoría informática en seguridad de la información se halla sustentada en los estándares de calidad como la ISO 27001, que define controles para una gestión de riesgo y protección de datos (ISO, 2022). A su vez, dicha auditoría podría utilizarse para auditar el funcionamiento de los sistemas de seguridad e identificar vulnerabilidades potenciales. La auditoría informática resulta clave, por otro lado, en el cumplimiento de la normativa como el GDPR puesto que permite verificar que las organizaciones están aplicando las medidas que resulten adecuadas para la protección de datos personales (Pandit et al., 2024). En el contexto ecuatoriano la aplicación de auditorías informáticas ha resultado de gran relevancia para mejorar la seguridad de la información en instituciones públicas y privadas. Los trabajos en la temática en Ecuador han constatado que las auditorías informáticas basadas en la ISO 27001 mejoran los controles internos y la gestión de riesgos (Chagmana Pomaquero, 2022; Ramírez Coello, 2023); la implementación de políticas de seguridad de la información posibilita establecer directrices claras que contribuyen con la protección de datos personales y con el cumplimiento normativo (Mullo-Pilamunga & Camero-Berrones, 2025). En definitiva la auditoría informática es una herramienta clave de la seguridad de la información y el cumplimiento normativo.

4. Desafíos en la implementación de normativas y auditorías

A pesar de que se han logrado avances significativos en la protección de datos, así como en la auditoría informática, su implementación presenta una serie de dificultades de las cuales hemos mencionado algunas: entre los problemas más importantes se encuentra la falta de formación de

las organizaciones, lo cual complica la adopción de estándares internacionales y el cumplimiento de las leyes. Por otro lado, la dificultad de integrar las regulaciones internacionales y las regulaciones nacionales, sobre todo en aquellos contextos donde las regulaciones todavía están en un proceso de consolidación (Asamblea Nacional del Ecuador, 2021), ya que necesitará incluir un esfuerzo extra para poder adaptarse a la realidad organizacional.

También, otro de los problemas importantes incluye la gestión de riesgos, puesto que el crecimiento exponencial tanto de las tecnologías de la información como de las nuevas amenazas digitales requiere que los sistemas de seguridad sean actualizados constantemente (Flores & Perugachi, 2023). En este sentido, la auditoría informática debe realizarse de forma permanente.

Por otro lado, la implementación de sistemas de gestión de seguridad conlleva varios costes y por eso la implementación de estos sistemas puede limitarse en organizaciones pequeñas y medianas (Mullo-Pilamunga & Camero-Berrones, 2025).

Finalmente, cabe resaltar que la protección de datos puede suponer retos éticos que giran en torno al uso de la información y la privacidad de los usuarios; por lo cual, hemos de ser responsables en la gestión de datos (Pandit et al., 2024).

En definitiva, los desafíos relacionados con la implementación de normativas y auditorías hacen necesario adoptar un enfoque integral en el que hemos de centrar la formación, la inversión y la gestión del cambio.

5. Conclusiones

La protección de datos y la normativa específica para las auditorías informáticas constituyen fundamentos básicos para la gestión de la seguridad de la información, en esta era digital que vivimos. El análisis realizado ha mostrado que la combinación de normas internacionales que pueden ser utilizadas como la ISO 27001 o la Ley Orgánica de Protección de Datos Personales, mejora los sistemas de control y el cumplimiento normativo.

Se ha podido determinar que la auditoría informática cumple un papel fundamental a la hora de determinar los riesgos y mejorar los controles internos de forma que contribuyan al reforzamiento de la seguridad de la información. Así mismo, el empleo de metodologías basadas en normas internacionales permite la puesta en práctica de las mejores prácticas de gestión de datos.

Sin embargo, la puesta en práctica de la normativa expuesta comporta unas dificultades importantes, especialmente en lo que respecta la capacitación, los costes y la adaptación organizativa. Además, la auditoría informática se enfrenta a un constante cambio de las condiciones de ataque que exigen la actualización de los sistemas de seguridad y de los procesos de auditoría.

La protección de datos también plantea cuestiones éticas que deben ser contempladas en la gestión de la información, respetando así la privacidad y los derechos de las personas.

En definitiva, la auditoría informática y la protección de datos constituyen una posibilidad de reforzar la seguridad de la información si se lleva a cabo de una forma estratégica, ética y alineada con las normativas existentes.

Bibliografía

Asamblea Nacional del Ecuador. (2021). *Ley Orgánica de Protección de Datos Personales*.

Chagmana Pomaquero, R. L. (2022). *Auditoría informática aplicando la norma ISO 27001 para optimizar la seguridad de la información*. Universidad Técnica de Ambato.

Flores, D. A., & Perugachi, R. (2023). *A GDPR-compliant risk management approach based on threat modelling and ISO 27005.*

Hjerppe, K., Ruohonen, J., & Leppänen, V. (2019). *The General Data Protection Regulation: Requirements, architectures, and constraints.*

Mullo-Pilamunga, X., & Camero-Berrones, R. (2025). *Políticas de seguridad de la información según la norma ISO 27001 en Ecuador*.

Organización Internacional de Normalización (ISO). (2022). *ISO/IEC 27001:2022 Information security*

management systems — Requirements.

Organización Internacional de Normalización (ISO). (2023). *ISO/IEC 27701: Privacy Information Management*.

Pandit, H. J., Lindquist, J., & Krog, G. P. (2024). *Implementing ISO privacy standards and GDPR compliance frameworks*.

Ramírez Coello, N. B. (2023). *Auditoría informática en la seguridad de la información según la ISO 27001 en empresas comerciales*. Universidad Laica Eloy Alfaro de Manabí.

Superintendencia de Protección de Datos Personales. (2025). *Guía de gestión de riesgos y evaluación de impacto del tratamiento de datos personales*.