Artículo de Investigación Original

El rol de la auditoría informática en la era de la protección de datos personales en Ecuador

The role of IT auditing in the era of personal data protection in Ecuador

Luis Lucero[0009-0007-1313-1922]
Universidad de Buenos Aires, Buenos Aires, Argentina
l.lucero@gmx.com

CITA EN APA:
Lucero, L. (2023). El rol de la auditoría informática en la era de la protección de datos personales en Ecuador. Technology Rain Journal, 2(2), e17. https://technologyrain.com.ar/index.php/trj/article/view/17

Recibido: 28-04-2023
Aceptado: 11-05-2023
Publicado: 01-07-2023

Technology Rain Journal
ISSN: 2953-464X

Resumen. La auditoría informática es un proceso de control que surge como un órgano de supervisión en instituciones estatales y privadas. Inicialmente, se enfocaba en aspectos económico-financieros, evaluando la integridad y veracidad de la información financiera y contable, y garantizando el cumplimiento de normas y regulaciones. La auditoría informática, por otro lado, tiene como objetivo evaluar y analizar los sistemas y procesos informáticos de una organización, buscando garantizar su integridad, confiabilidad y seguridad. Se lleva a cabo mediante actividades como la revisión de controles internos, evaluación de riesgos, análisis de infraestructura tecnológica y cumplimiento de normativas vigentes. La auditoría informática también se preocupa por la gestión de la información y la eficiencia de los sistemas informáticos. Su importancia radica en la protección de recursos informáticos, cumplimiento de políticas y normas, gestión de la información y mejora de la eficiencia de los sistemas. Se analizó los cambios que han surgido en el ámbito de la auditoria informática en relación a la implementación de la ley de protección de datos en Ecuador.

Palabras Clave: Auditoría Informática, protección de datos, gestión de la información.

Abstract. Computer auditing is a control process that emerged as a supervisory body in state and private institutions. Initially, it focused on economic-financial aspects, evaluating the integrity and veracity of financial and accounting information, and ensuring compliance with rules and regulations. Computer auditing, on the other hand, aims to evaluate and analyze an organization's computer systems and processes, seeking to ensure their integrity, reliability and security. It is carried out through activities such as the review of internal controls, risk assessment, analysis of technological infrastructure and compliance with current regulations. IT auditing is also concerned with information management and the efficiency of IT systems. Its importance lies in the protection of IT resources, compliance with policies and standards, information management and improvement of system efficiency. The changes that have arisen in the field of computer auditing in relation to the implementation of the data protection law in Ecuador were analyzed.

Keywords: IT Audit, data protection, information management.

1. INTRODUCCIÓN

La auditoría informática desempeña un papel crucial en la protección de datos personales. Según Reascos Velastegui (2019), la auditoría informática se caracteriza por ser un proceso sistemático y metódico que busca garantizar la integridad, confiabilidad y seguridad de los sistemas informáticos y la información manejada por una organización. Esto implica llevar a cabo revisiones exhaustivas de los controles internos para identificar posibles vulnerabilidades y evaluar los riesgos asociados al uso de la tecnología de la información.

En el contexto actual, con el crecimiento exponencial de las redes sociales y su impacto en la vida cotidiana, la seguridad y protección de los datos personales en estos entornos digitales se ha vuelto cada vez más importante. Tanto las personas individuales como las empresas y organizaciones que operan en línea están expuestas a ciberataques que buscan obtener acceso no autorizado a perfiles y explotar información con fines maliciosos. Esta vulnerabilidad plantea un desafío para la protección de datos y la seguridad en redes sociales.

La investigación sobre ciberataques en sitios de redes sociales y la protección de datos personales revela que no solo las personas individuales están expuestas a estos ataques, sino también las empresas y organizaciones que operan en línea (Escobar-Macías & Alvarez-Galarza, 2022). Con el aumento en el uso de las redes sociales y su impacto en la vida cotidiana, es fundamental garantizar la seguridad y protección de los datos personales en estos entornos digitales.

Diversas investigaciones han destacado la importancia de abordar los ciberataques en redes sociales y proteger los datos personales. Los estudios han analizado la auditoría informática como un proceso sistemático y metódico que busca garantizar la integridad, confiabilidad y seguridad de los sistemas informáticos y la información manejada por una organización (Reascos Velastegui, 2019). Además, se han examinado las normativas y regulaciones vigentes en materia de protección de datos para evaluar el cumplimiento de las leyes y regulaciones aplicables en relación con la recolección, almacenamiento, procesamiento y transmisión de datos personales.

La implementación de la ley de protección de datos en Ecuador y la necesidad de adaptar la auditoría informática a estos cambios han motivado al autor a investigar los avances y modificaciones en el ámbito de la auditoría informática en relación con la protección de datos en redes sociales. El autor se ha interesado en analizar cómo la auditoría informática puede fortalecer la seguridad y protección de los datos personales en estos entornos digitales y cómo puede contribuir al cumplimiento de los requisitos legales establecidos en Ecuador.

El objetivo de esta investigación es analizar los cambios que han surgido en el ámbito de la auditoría informática en relación a la implementación de la ley de protección de datos en Ecuador. Se busca comprender cómo la auditoría informática puede fortalecer la seguridad y protección de

los datos personales en redes sociales, identificar posibles deficiencias en los procedimientos y controles existentes, y formular recomendaciones para mitigar los riesgos de ciberataques.

En esta investigación se llevará a cabo un análisis exhaustivo de la auditoría informática en el contexto de la protección de datos en redes sociales, específicamente en relación con la implementación de la ley de protección de datos en Ecuador. Se examinarán los cambios y adaptaciones que se han realizado en el ámbito de la auditoría informática para cumplir con los requisitos legales y proteger los datos personales en redes sociales. A partir de revisiones exhaustivas y análisis de los controles internos, se identificarán posibles vulnerabilidades y se propondrán medidas de seguridad adecuadas para mitigar los riesgos de ciberataques (Reascos Velastegui, 2019).

2. METODOLOGÍA

El presente artículo científico emplea una metodología descriptiva con el propósito de brindar una panorámica general y una síntesis de la literatura disponible acerca de la auditoría informática. Los datos utilizados en este estudio se adquieren mediante la revisión de artículos científicos y la exploración de bases de datos en línea, haciendo uso de palabras clave relevantes.

Se lleva a cabo un análisis exhaustivo de los artículos seleccionados con el fin de identificar temas fundamentales y extraer información pertinente. No se recolectan datos primarios ni se realizan experimentos en este tipo de investigación. El enfoque principal de este estudio es reunir y organizar el conocimiento existente, así como identificar tendencias y brechas en la investigación. Los resultados obtenidos pueden servir como base para futuras investigaciones y como fuente de información para profesionales y académicos interesados en la auditoría informática.

3. CONTEXTULIZACIÓN

La Auditoría Informática

1. **Auditoría:** según Deream Arom Jimenez Ortiz y Ayala (2019), la auditoría es un proceso de control que surge como un órgano de supervisión en instituciones estatales y privadas. Inicialmente, su función se centraba en aspectos económico-financieros, como lo evidencian las peritaciones judiciales y las contrataciones de contables expertos por parte de bancos oficiales. La auditoría tiene como objetivo principal evaluar la integridad y veracidad de la información financiera y contable, así como garantizar el cumplimiento de las normas y regulaciones aplicables. En el proceso de auditoría, se utilizan técnicas de análisis, verificación y exposición de debilidades y disfunciones, y se pueden presentar recomendaciones en el informe final para abordar las deficiencias identificadas.

La auditoría se lleva a cabo de manera independiente, lo que significa que el auditor no tiene ninguna relación directa con la organización auditada y sus conclusiones no son vinculantes. Esto garantiza una evaluación imparcial y objetiva de la información financiera y contable de la organización. A través de la aplicación de técnicas rigurosas de auditoría, como pruebas de cumplimiento, pruebas sustantivas y revisión de controles internos, se busca identificar posibles errores, fraudes o irregularidades en los registros contables. Además, se evalúan los procedimientos y controles internos para determinar su efectividad y eficiencia.

2. **Auditoría Informática:** la auditoría informática se refiere a un proceso metódico y sistemático cuyo propósito principal es evaluar y analizar los sistemas y procesos informáticos de una organización (Bailon, 2019). Su objetivo es garantizar la integridad, confiabilidad y seguridad de la infraestructura tecnológica y la información manejada por la organización (Imbaquingo, 2020).

   Según Imbaquingo et al (2020), esta auditoría implica una serie de actividades, que incluyen la revisión de los controles internos, la evaluación de los riesgos asociados al uso de la tecnología de la información, el análisis de la infraestructura tecnológica, la revisión de los procedimientos de seguridad y el cumplimiento de las normativas y regulaciones vigentes.

   Durante el proceso de auditoría informática, se llevan a cabo diversas etapas, como la recopilación y análisis de información, la identificación de vulnerabilidades y debilidades, la evaluación de los controles existentes, la formulación de recomendaciones para mejorar la seguridad y eficiencia de los sistemas informáticos, y la emisión de informes detallados con los resultados obtenidos (Albarrán et al, 2020).

   Es importante resaltar que la auditoría informática no se enfoca únicamente en aspectos técnicos, sino que también considera la gestión de la información, el cumplimiento de políticas y normas internas, así como la protección de la privacidad y confidencialidad de los datos.

3. **Metodología de la Auditoría Informática:** Según Palomino Sysoeva, D. A., & Villegas Rojas, C. A. (2022), propone una metodología flexible y escalable para llevar a cabo la auditoría informática interna en la Universidad Andina del Cusco. Esta metodología consta de cuatro fases que orientan todo el proceso de auditoría:

   En la primera fase, se establece el contacto con los responsables y colaboradores de la universidad para recopilar información relevante sobre la infraestructura tecnológica, los sistemas informáticos y los procesos relacionados. También se recaban los aspectos generales necesarios para comprender el entorno y los objetivos de la auditoría.

   La segunda fase se centra en la planificación detallada de la auditoría informática. Aquí se definen los objetivos específicos, el alcance de la auditoría, los recursos necesarios y se elabora

un cronograma de actividades. Además, se identifican los riesgos asociados y se determinan las técnicas de auditoría adecuadas para evaluarlos.

En la tercera fase, se lleva a cabo el trabajo de campo de la auditoría. Se recopila y analiza la información pertinente, se realizan pruebas y se evalúan los controles internos existentes. Se identifican posibles vulnerabilidades y debilidades en los sistemas informáticos, y se formulan recomendaciones para mejorar la seguridad y eficiencia de los mismos. Durante todo el proceso, se garantiza la confidencialidad y la integridad de la información.

En la fase final, se elabora el informe final de la auditoría informática. En este informe se presentan de manera clara y concisa los hallazgos, las recomendaciones y las conclusiones derivadas del proceso de auditoría. Se hace hincapié en la importancia de que las recomendaciones sean prácticas y se prioricen en función de su impacto y riesgo. El informe se entrega a la dirección de la universidad para su revisión y toma de decisiones.

Además, se contempla la posibilidad de agregar una fase de seguimiento y control del cumplimiento de las recomendaciones emitidas durante la auditoría, lo cual será evaluado por la comisión auditora. La metodología se basa en los principios de COBIT 5 y los estándares generales de ISACA para garantizar la calidad y la ética en todo el proceso de auditoría.

4. **Importancia de La Auditoria Informática:** Según Deream Arom Jimenez Ortiz, & Ayala, J. C. (2019), la Auditoría Informática desempeña un papel de vital importancia en el entorno empresarial actual, donde la tecnología de la información se ha convertido en una parte fundamental de las operaciones y procesos de las organizaciones. Su objetivo principal radica en garantizar la integridad, confiabilidad y seguridad de los sistemas informáticos y la información que se maneja en ellos.

   En primer lugar, la Auditoría Informática cumple un rol fundamental en la protección de los recursos informáticos de una organización. Esto implica evaluar y analizar los sistemas y procesos tecnológicos para identificar posibles vulnerabilidades y debilidades que puedan poner en riesgo la seguridad de la infraestructura tecnológica y la información almacenada en ella. Mediante la detección de riesgos, se pueden implementar medidas y controles necesarios para prevenir y mitigar posibles amenazas.

   Además, la Auditoría Informática contribuye a asegurar el cumplimiento de políticas, normas y regulaciones internas y externas. Esto implica evaluar si los sistemas y procesos informáticos están alineados con las directrices y estándares establecidos, así como verificar si se cumplen los requisitos legales y de seguridad. De esta manera, se garantiza que la organización opere de acuerdo con las normas y se evitan posibles sanciones y consecuencias negativas.

   Otro aspecto importante de la Auditoría Informática es su enfoque en la gestión de la información. Esto implica evaluar la calidad, precisión, confidencialidad e integridad de los

datos manejados por los sistemas informáticos. Se busca asegurar que la información esté disponible cuando sea necesaria, sea precisa y confiable, y esté protegida contra accesos no autorizados. Esto se logra a través de la revisión de los controles de acceso, la implementación de medidas de seguridad adecuadas y la realización de pruebas de validación.

Además, la Auditoría Informática también se preocupa por la eficiencia y eficacia de los sistemas informáticos. Esto implica evaluar la adecuada utilización de los recursos, el rendimiento de los sistemas, la optimización de los procesos y la identificación de posibles mejoras. Se busca garantizar que los sistemas informáticos cumplan con su propósito de apoyar las operaciones de la organización de manera eficiente y efectiva.

5. **Hallazgos:** se refiere a la identificación de una situación, hecho o condición que se considera relevante y que requiere atención o acción por parte de la organización auditada. Estos hallazgos pueden ser positivos, cuando se encuentran prácticas o controles efectivos que contribuyen al cumplimiento de los objetivos de la auditoría, o negativos, cuando se detectan debilidades, deficiencias o incumplimientos en los sistemas informáticos y procesos relacionados. Los hallazgos en auditoría informática se basan en el análisis y evaluación de la infraestructura tecnológica, los controles internos, los procedimientos de seguridad, el cumplimiento de normativas y regulaciones, y otros aspectos relevantes para garantizar la integridad, confiabilidad y seguridad de los sistemas informáticos y la información manejada por la organización (Deream Arom Jimenez Ortiz, & Ayala, J. C.,2019).

   Una vez identificados los hallazgos, se documentan en el informe de auditoría informática, donde se describen de manera clara y concisa, se presentan las evidencias recopiladas durante la auditoría y se proporcionan recomendaciones para abordar y solucionar los problemas identificados. Estos hallazgos son de vital importancia para la toma de decisiones de la organización auditada, ya que les permiten mejorar sus prácticas de seguridad, eficiencia y cumplimiento normativo en el ámbito informático (Deream Arom Jimenez Ortiz, & Ayala, J. C.,2019).

Protección de datos personales en Ecuador: La protección de datos personales es un derecho fundamental reconocido por la Constitución del Ecuador y por diversos instrumentos internacionales. Este derecho implica que las personas tienen el poder de controlar la información que les concierne, así como el uso que se le da a la misma por parte de terceros, sean estos públicos o privados. La protección de datos personales busca garantizar la autodeterminación informativa, la intimidad, la honra y la reputación de las personas frente al tratamiento de sus datos personales (LOPDP, 2021).

Ecuador cuenta con una normativa específica sobre protección de datos personales, que es la Ley Orgánica de Protección de Datos Personales, publicada en el Registro Oficial el 17 de febrero de 2021. Esta ley establece los principios, derechos, obligaciones y procedimientos para regular el tratamiento de datos personales en el país, así como las autoridades competentes para su aplicación y control. La ley también prevé la creación de un Registro Nacional de Protección de Datos Personales, que será administrado por el Consejo de Participación Ciudadana y Control Social (LOPDP, 2021).

La existencia de esta ley demuestra el compromiso de Ecuador en proteger la privacidad y los derechos de las personas en el entorno digital. Proporciona un marco legal claro y establece responsabilidades para las organizaciones que recopilan, procesan y almacenan datos personales. Esto brinda a los individuos un mayor control sobre su información personal y establece pautas claras para el uso adecuado y seguro de los datos.

Además, la Ley Orgánica de Protección de Datos Personales también fomenta la conciencia y la cultura de protección de datos en la sociedad ecuatoriana. Al establecer los principios y derechos fundamentales en materia de protección de datos, se promueve una mayor responsabilidad por parte de las organizaciones y se fomenta la transparencia en el manejo de la información personal. Esto contribuye a fortalecer la confianza de los individuos en el uso de los servicios digitales y a garantizar un entorno seguro para el intercambio de información.

1. **Ley de protección de datos personales:** la ley de protección de datos personales ecuador es una norma jurídica que tiene como objetivo garantizar el derecho fundamental de las personas a la autodeterminación informativa, es decir, a decidir libremente sobre el uso y destino de sus datos personales. Esta ley establece los principios, derechos, obligaciones y procedimientos que deben observar los responsables y encargados del tratamiento de datos personales, así como las autoridades competentes para su protección y control. La ley de protección de datos personales ecuador reconoce a los titulares de los datos personales el derecho de acceso, rectificación, cancelación, oposición, portabilidad e información sobre sus datos, así como el derecho a no ser objeto de decisiones automatizadas que afecten su esfera jurídica o personal. Asimismo, la ley de protección de datos personales ecuador establece las medidas de seguridad que deben adoptar los responsables y encargados del tratamiento de datos personales para evitar su pérdida, alteración, acceso no autorizado o uso indebido. La ley de protección de datos personales ecuador también regula las transferencias internacionales de datos personales, las infracciones y sanciones administrativas, así como las acciones judiciales y extrajudiciales que pueden ejercer los titulares de los datos personales en caso de vulneración de sus derechos (LOPDP, 2021).

2. **Obligaciones de las empresas que tratan los datos:** Según la Ley Orgánica de Protección de Datos Personales (LOPDP, 2021), las empresas que tratan datos personales en Ecuador tienen una serie de obligaciones que deben cumplir. Estas obligaciones están diseñadas para proteger los derechos de los ciudadanos ecuatorianos y garantizar un tratamiento adecuado y seguro de sus datos. Algunas de estas obligaciones incluyen:
    - Obtener el consentimiento expreso, previo, libre e informado de los titulares de los datos para su tratamiento, a menos que existan excepciones previstas en la ley. Esto significa que las empresas deben obtener un consentimiento claro y específico de los individuos antes de recopilar, procesar o utilizar sus datos personales.
    - Informar a los titulares de los datos sobre la finalidad, el alcance, la duración y el responsable del tratamiento de sus datos. Las empresas deben ser transparentes y proporcionar información clara a los individuos sobre cómo se utilizarán sus datos personales, quién será responsable de su tratamiento y durante cuánto tiempo se conservarán.
    - Garantizar la seguridad, confidencialidad e integridad de los datos personales. Las empresas deben implementar medidas técnicas y organizativas adecuadas para proteger los datos contra pérdida, alteración, acceso no autorizado o uso indebido. Esto implica el uso de medidas de seguridad como el cifrado de datos, el control de acceso y la protección contra amenazas cibernéticas.
    - Respetar los principios de licitud, finalidad, proporcionalidad, calidad, transparencia y responsabilidad en el tratamiento de los datos personales. Esto implica que las empresas deben cumplir con los principios éticos y legales establecidos en la ley al tratar los datos personales de los individuos.
    - Notificar tanto a los titulares de los datos como a la autoridad competente en caso de que ocurra una violación de seguridad que afecte los datos personales. Las empresas deben tomar las medidas necesarias para informar a los individuos y a las autoridades pertinentes en caso de que se produzca una brecha de seguridad que comprometa la privacidad de los datos.
    - Cumplir con las disposiciones y sanciones establecidas por la ley y el reglamento en materia de protección de datos personales. Esto implica que las empresas deben cumplir con todas las regulaciones y normativas establecidas por la LOPDP y enfrentar posibles sanciones en caso de incumplimiento.

    Estas obligaciones establecidas por la Ley Orgánica de Protección de Datos Personales buscan garantizar que las empresas en Ecuador traten los datos personales de manera responsable,

ética y segura, protegiendo así los derechos y la privacidad de los ciudadanos. Al cumplir con estas obligaciones, las empresas contribuyen a generar confianza en el uso y la gestión de los datos personales en el entorno digital.

Auditoría informática y protección de datos personales: Según Corredera de Colsa, L. E., & García Fernández, F. (2019), en cada país existe legislación vigente para el control, tratamiento y transmisión de la información personal. Estos controles establecen ciertas obligaciones que la organización debe cumplir en cuanto a la protección de datos personales. En el contexto de una auditoría informática, es fundamental tener en cuenta esta legislación y evaluar si los sistemas y procesos de la organización están cumpliendo con los requisitos establecidos.

En el caso específico de analizar un sistema que incumple la normativa de protección de datos, la auditoría informática se convierte en una herramienta clave para identificar y abordar esta problemática. El incumplimiento de la normativa puede manifestarse en diversas formas, como el acceso no autorizado a datos personales, la falta de controles adecuados para garantizar la confidencialidad y la integridad de la información, o la transmisión insegura de datos sensibles.

Al realizar la auditoría informática, se lleva a cabo un análisis exhaustivo del sistema, identificando las áreas en las que se produce el incumplimiento de la normativa. Esto implica evaluar la implementación de medidas de seguridad, la configuración de los sistemas, el acceso a los datos y la gestión de los registros, entre otros aspectos relevantes.

Una vez identificadas las deficiencias, la auditoría informática debe formular recomendaciones y acciones correctivas para abordar el incumplimiento de la normativa. Estas recomendaciones pueden incluir la mejora de los controles de acceso, la implementación de medidas de seguridad adicionales, la revisión de los procedimientos de gestión de datos y la capacitación del personal en materia de protección de datos.

Es importante que la auditoría informática documente detalladamente los hallazgos relacionados con el incumplimiento de la normativa de protección de datos y sus implicaciones para la organización. Esto permitirá a la dirección tomar decisiones informadas y tomar las medidas necesarias para corregir las deficiencias encontradas.

Beneficios de realizar auditorías informáticas regulares para garantizar la seguridad de los datos personales: la realización de auditorías informáticas regulares para garantizar la seguridad de los datos personales es un aspecto de suma importancia en la gestión de la información en la actualidad. Según Deream Arom Jimenez Ortiz y Ayala J. C. (2019), esta práctica adquiere un valor significativo al proporcionar los controles necesarios y suficientes que contribuyen al apropiado desempeño de los sistemas de información, asegurando así la confiabilidad y seguridad de estos.

En un entorno cada vez más digitalizado y con constantes avances tecnológicos, es imprescindible contar con sistemas de información confiables y seguros para proteger los datos personales de los individuos. Las auditorías informáticas se convierten en una herramienta fundamental para lograr este objetivo, ya que permiten evaluar de manera sistemática los sistemas y procesos informáticos de una organización en busca de posibles vulnerabilidades, fallas en los controles y riesgos asociados a la protección de los datos personales.

La identificación de estas vulnerabilidades y riesgos mediante las auditorías informáticas brinda a la organización la oportunidad de implementar medidas preventivas y correctivas de manera proactiva. Esto implica fortalecer los controles de seguridad existentes, mejorar las políticas y procedimientos internos, y adoptar tecnologías más avanzadas para garantizar la integridad, confidencialidad y disponibilidad de la información personal.

Asimismo, las auditorías informáticas ayudan a las organizaciones a cumplir con las normativas y regulaciones vigentes en materia de protección de datos personales. En un contexto donde las leyes y regulaciones sobre privacidad y protección de datos están en constante evolución, las auditorías informáticas se convierten en una herramienta indispensable para verificar si la organización está cumpliendo con los requisitos legales y éticos establecidos. Esto incluye aspectos como la obtención del consentimiento adecuado para el procesamiento de datos, la implementación de medidas de seguridad técnicas y organizativas apropiadas, y la notificación de brechas de seguridad en caso de producirse.

Además, las auditorías informáticas contribuyen a la detección temprana de posibles incidentes de seguridad y amenazas cibernéticas. Al evaluar de manera sistemática los sistemas informáticos, se pueden identificar patrones o comportamientos anómalos que podrían indicar la presencia de ataques o intrusiones no autorizadas. Esto permite tomar medidas inmediatas para mitigar el impacto y minimizar los riesgos asociados con la seguridad de los datos personales.

El papel clave de la auditoría informática en la prevención de violaciones a la ley de protección de datos: la auditoría informática desempeña un papel importante en la prevención de violaciones a la ley de protección de datos ya que, según Ramos, M. A. (1996), al constatar los accesos autorizados en cumplimiento de las políticas de la entidad. Para el adecuado control interno y una posterior auditoría efectiva, es fundamental contar con registros que permitan identificar quién ha accedido a qué información, así como quién ha realizado modificaciones o eliminaciones y cuándo, e incluso desde qué ubicación se ha llevado a cabo dicha actividad.

La auditoría informática se enfoca en evaluar y verificar la implementación de medidas de seguridad que aseguren el cumplimiento de la normativa de protección de datos. A través de la revisión

exhaustiva de los controles y procedimientos existentes, se busca identificar posibles vulnerabilidades y riesgos que podrían dar lugar a violaciones de la ley.

La importancia de contar con registros detallados de los accesos y acciones realizadas radica en la capacidad de rastrear y responsabilizar a los individuos involucrados en caso de cualquier incidencia. Los registros de auditoría permiten identificar patrones sospechosos, detectar actividades no autorizadas o inapropiadas, y tomar medidas correctivas de manera oportuna para evitar cualquier violación a la ley de protección de datos.

Asimismo, la auditoría informática proporciona una visión integral de los sistemas y procesos tecnológicos de una organización, asegurando que los controles implementados sean efectivos y estén alineados con las regulaciones vigentes. Además, evalúa el cumplimiento de las políticas de seguridad establecidas y la efectividad de las medidas de protección de datos implementadas.

4. DISCUSIÓN

Los resultados presentados en este artículo de revisión resaltan la importancia de la auditoría informática en la protección de datos personales. La auditoría informática desempeña un papel fundamental al evaluar y analizar de manera sistemática los sistemas y procesos informáticos de una organización. Su objetivo principal es garantizar la integridad, confiabilidad y seguridad de la infraestructura tecnológica y la información manejada. A través de la identificación de posibles vulnerabilidades y debilidades en los sistemas, la auditoría informática permite implementar medidas y controles necesarios para prevenir y mitigar amenazas. Asimismo, contribuye al cumplimiento de políticas, normas y regulaciones tanto internas como externas, asegurando que los sistemas informáticos estén alineados con los estándares establecidos y cumpliendo con los requisitos legales y de seguridad.

En el contexto de la protección de datos personales en Ecuador, se reconoce que es un derecho fundamental respaldado por la legislación vigente. La Ley Orgánica de Protección de Datos Personales establece los principios, derechos, obligaciones y procedimientos para regular el tratamiento de datos personales en el país. La auditoría informática se convierte en una herramienta esencial para garantizar el cumplimiento de esta normativa, al evaluar la gestión de la información, la confidencialidad y la integridad de los datos manejados por los sistemas informáticos. Además, la auditoría informática desempeña un papel crucial al identificar posibles riesgos y vulnerabilidades en el manejo de datos personales en distintas plataformas digitales. Esto permite tomar medidas proactivas para fortalecer la seguridad y protección de los datos, tanto para los individuos como para las organizaciones que operan en línea.

5. RESULTADOS

ASPECTO	ANTES DE LA IMPLEMENTACIÓN DE LA LEY DE PROTECCIÓN DE DATOS	DESPUÉS DE LA IMPLEMENTACIÓN DE LA LEY DE PROTECCIÓN DE DATOS
Alcance de la auditoría	La auditoría informática se centraba en la evaluación de los sistemas informáticos y las medidas de seguridad técnicas. La revisión de los controles de protección de datos personales no era un enfoque prioritario.	La auditoría informática amplía su alcance para incluir una evaluación exhaustiva de los controles de protección de datos personales, asegurando el cumplimiento de las regulaciones establecidas por la ley de protección de datos.
Evaluación de riesgos	La evaluación de riesgos no tenía un enfoque específico en los riesgos asociados a la protección de datos personales.	Se incorpora una evaluación detallada de los riesgos asociados a la protección de datos personales, considerando aspectos como la confidencialidad, integridad y disponibilidad de la información personal en redes sociales.
Revisión de políticas y procedimientos	Las políticas y procedimientos relacionados con la protección de datos personales no eran una prioridad en la revisión de la auditoría informática.	Se lleva a cabo una revisión exhaustiva de las políticas y procedimientos existentes para garantizar el cumplimiento de las regulaciones de protección de datos y se recomiendan mejoras y ajustes según sea necesario.
Cumplimiento normativo	No se realizaban evaluaciones específicas del cumplimiento normativo en relación con la protección de datos personales.	Se incorpora una evaluación detallada del cumplimiento normativo en relación con la protección de datos personales, asegurando que la organización cumpla con las leyes y regulaciones establecidas por la ley de protección de datos en Ecuador.
Reporte y recomendaciones	Las recomendaciones se centraban en la mejora de la seguridad de los sistemas informáticos en general.	Las recomendaciones se enfocan en fortalecer los controles de protección de datos personales, implementar medidas adicionales de seguridad y garantizar el cumplimiento de las regulaciones establecidas por la ley de protección de datos.

Elaborado por : El autor

6. CONCLUSIONES

- La auditoría informática ha ampliado su alcance para incluir una evaluación exhaustiva de los controles de protección de datos personales. Anteriormente, el enfoque se centraba en la evaluación de sistemas informáticos y medidas de seguridad técnicas. Ahora, se reconoce la importancia de revisar y evaluar los controles específicos relacionados con la protección de datos personales en redes sociales.

- La evaluación de riesgos se ha vuelto más integral, considerando los riesgos asociados a la confidencialidad, integridad y disponibilidad de la información personal en redes sociales. Esto se debe a la necesidad de identificar y mitigar los riesgos específicos que surgen de la interacción de las personas y las organizaciones en estos entornos digitales.
- Existe un mayor énfasis en la revisión y mejora de políticas y procedimientos relacionados con la protección de datos personales. La auditoría informática se encarga de evaluar el cumplimiento normativo en relación a la recolección, almacenamiento, procesamiento y transmisión de datos personales, asegurando que las organizaciones cumplan con las leyes y regulaciones establecidas por la ley de protección de datos en Ecuador.

REFERENCIAS

Albarrán, S., Pérez, J., Salgado, M. & Valero, L. (2020). Las Metodologías de la Auditoría Informática y su relación con Buenas Prácticas y Estándares. Ideas en Ciencias de la Ingeniería, 1(1), pp. 49-70. https://ideasencienciasingenieria.uaemex.mx/article/view/14591

Bailon, W. (2019). Auditoria informática al control y mantenimiento de una infraestructura tecnológica. CIENCIAMATRIA, 5(1), 73-87. https://doi.org/10.35381/cm.v5i1.248

Corredera de Colsa, L. E., & García Fernández, F. (2019). Auditoría informática. https://gredos.usal.es/bitstream/handle/10366/139644/BISITE_Corredera_Garc%c3%ada_Auditor%c3%adainform%c3%a1tica.pdf?sequence=1&isAllowed=y

Deream Arom Jimenez Ortiz, & Ayala, J. C. (2019). Estado del Arte de la Auditoría informática y su importancia para las empresas.Universidad Nacional de Piura, Escuela profesional de contabilidad , Piura. Perú. Obtenido de https://repositorio.unp.edu.pe/bitstream/handle/UNP/1971/FCC-JIM-ORT-2019.pdf?sequence=1&isAllowed=y

Escobar-Macías, A. D., & Alvarez-Galarza, M. D. (2022). Análisis de ciberataques sobre el uso de redes sociales en relación a la protección de datos personales en Ecuador. Domino De Las Ciencias, 8(1), 1070–1079. https://doi.org/10.23857/dc.v8i1.2622

Imbaquingo, D., Díaz, J., Saltos, T., Arciniega, S., De la Torre, J. & Jácome, J. (2020). Análisis de las principales dificultades en la auditoría informática: una revisión sistemática de literatura. Revista Ibérica de Sistemas e Tecnologias de Informação, N.º E32, pp. 427-440. https://www.proquest.com/openview/8d965b8c754de2de0771f5153b163d33/1?pq-origsite=gscholar&cbl=1006393 g

LOPDP. Ley 0. Registro Oficial Suplemento 459 de 26-may.-2021. Estado: Vigente. https://www.finanzaspopulares.gob.ec/wp-content/uploads/2021/07/ley_organica_de_proteccion_de_datos_personales.pdf

Palomino Sysoeva, D. A., & Villegas Rojas, C. A. (2022). Propuesta de una metodología de auditoría informática para la oficina de Auditoría Interna de la Universidad Andina del Cusco. https://repositorio.uandina.edu.pe/bitstream/handle/20.500.12557/4998/Daniela_Carolina_Tesis_bachiller_2022.pdf?sequence=1&isAllowed=y

Ramos, M. A. (1996). El papel clave de la auditoría informática en la prevención de violaciones a la ley de protección de datos. Informática y derecho: Revista iberoamericana de derecho informático, 12-15 (Ejemplar dedicado a: II

Congreso Internacional de Informática y Derecho. Actas (volumen II)), 983-992. https://dialnet.unirioja.es/descarga/articulo/248905.pdf

Reascos Velastegui, D. X. (2019). Auditoría informática al Departamento de Tecnología de la Información y Comunicación del Hospital Provincial General Docente Riobamba (Bachelor's thesis, Escuela Superior Politécnica de Chimborazo). http://dspace.espoch.edu.ec/bitstream/123456789/11605/1/82T00950.pdf