Ciencia Latina Revista Científica Multidisciplinar, Ciudad de México, México.
ISSN 2707-2207 / ISSN 2707-2215 (en línea), marzo-abril 2025,
Volumen 9, Número 2.

https://doi.org/10.37811/cl_rcm.v9i2

AUDITORÍA DE CONTROLES DE CIFRADO Y PROTECCIÓN DE LA INFORMACIÓN

AUDITORÍA DE CONTROLES DE CIFRADO Y PROTECCIÓN DE LA INFORMACIÓN

Jonnathan Raúl Flores Tunja
Instituto Superior Universitario Sucre

Carla Paulina Juiña Pillalaza
Instituto Superior Universitario Sucre

Nacimba Proaño Dennis Fernando
Instituto Superior Universitario Sucre

Franklin Marcelo Tandalla Quimbita
Instituto Superior Universitario Sucre

Alex Santiago Guanoquiza Guanoquiza
Instituto Superior Universitario Sucre

DOI: https://doi.org/10.37811/cl_rcm.v9i2.16856

Auditoría de controles de cifrado y protección de la información

Jonnathan Raúl Flores Tunja[1]
jflores@tecnologicosucre.edu.ec
https://orcid.org/0009-0005-9812-9156
Instituto Superior Universitario Sucre
Ecuador

Carla Paulina Juiña Pillalaza
cjuina@tecnologicosucre.edu.ec
https://orcid.org/0009-0006-6248-3396
Instituto Superior Universitario Sucre
Ecuador

Nacimba Proaño Dennis Fernando
dnacimba@tecnologicosucre.edu.ec
https://orcid.org/0009-0007-0791-5712
Instituto Superior Universitario Sucre
Ecuador

Franklin Marcelo Tandalla Quimbita
ftandalla@tecnologicosucre.edu.ec
https://orcid.org/0009-0003-7898-2657
Instituto Superior Universitario Sucre
Ecuador

Alex Santiago Guanoquiza Guanoquiza
aguanoquiza@tecnologicosucre.edu.ec
https://orcid.org/0009-0000-4121-9138
Instituto Superior Universitario Sucre
Ecuador

RESUMEN

El estudio titulado auditoría de controles de cifrado y protección de la información tiene como objetivo evaluar el nivel de seguridad de los datos, identificando posibles riesgos y deficiencias en su protección. Para ello, se basa en la norma ISO 27002, la cual establece controles específicos para garantizar la confidencialidad, integridad y disponibilidad de la información. Este trabajo se ha desarrollado tomando como base investigaciones previas en el área de auditoría de seguridad informática, con el propósito de estructurar una metodología efectiva que permita detectar vulnerabilidades y sugerir estrategias de mejora. Se han analizado modelos de auditoría utilizados en otras empresas, contrastando sus resultados con los obtenidos en esta investigación. El estudio incluye un análisis exhaustivo de los controles de seguridad implementados, enfocándose especialmente en el cifrado y la protección de información sensible, identificando vulnerabilidades potenciales en el acceso y almacenamiento de datos financieros y administrativos. A través de un proceso de auditoría sistemático, se revisan aspectos clave como la gestión de claves criptográficas, los procedimientos de respaldo y la aplicación de medidas de control recomendadas por normativas internacionales como la ISO 27001 y el NIST 800-53.

Palabras clave: derecho del ciberespacio, tecnología adecuada, gobernanza de internet (tesauro unesco)

[1] Autor principal.
Correspondencia: jonathankamergi@gmail.com

Auditoría de controles de cifrado y protección de la información

ABSTRACT

The study entitled audit of encryption controls and information protection aims to evaluate the level of data security, identifying possible risks and deficiencies in its protection. For this purpose, it is based on the ISO 27002 standard, which establishes specific controls to guarantee the confidentiality, integrity and availability of information. This work has been developed based on previous research in the area of computer security auditing, with the purpose of structuring an effective methodology to detect vulnerabilities and suggest improvement strategies. Audit models used in other companies have been analyzed, contrasting their results with those obtained in this research. The study includes an exhaustive analysis of the security controls implemented, focusing especially on encryption and protection of sensitive information, identifying potential vulnerabilities in the access and storage of financial and administrative data. Through a systematic audit process, key aspects such as cryptographic key management, backup procedures and the application of control measures recommended by international standards such as ISO 27001 and NIST 800-53 are reviewed.

***Keywords*:** cyberspace law; appropriate technology; internet governance (unesco thesaurus)

Artículo recibido 13 febrero 2025
Aceptado para publicación: 19 marzo 2025

INTRODUCCIÓN

En la actualidad, la protección de la información se ha convertido en una necesidad fundamental en los sistemas contables para las organizaciones que manejan grandes volúmenes de datos sensibles. Con el crecimiento de las tecnologías y la digitalización de procesos, las empresas enfrentan amenazas cibernéticas cada vez más avanzadas, lo que hace esencial la implementación de mecanismos de seguridad robustos, como el cifrado de datos. Este mecanismo asegura no solo la confidencialidad, sino también la integridad y disponibilidad de la información crítica.

El cifrado AES-256 ha emergido como uno de los algoritmos más utilizados y recomendados para la protección de datos, debido a su alta seguridad y eficiencia, particularmente en sectores clave como el financiero, la salud y las telecomunicaciones. Sin embargo, su implementación requiere una adecuada administración y supervisión, aspectos que, en muchos casos, no se llevan a cabo efectivamente, exponiendo a las organizaciones a riesgos de seguridad significativos, tales como accesos no autorizados o filtraciones de datos.

A pesar de la existencia de normativas como la Ley Orgánica de Protección de Datos y Garantía de los Derechos Digitales (LOPDGDD), el Reglamento General de Protección de Datos (RGPD) y la ISO 27001, muchas organizaciones enfrentan retos en la adecuada implementación de controles de cifrado y en la realización de auditorías que aseguren su cumplimiento. La falta de auditorías periódicas y la gestión inadecuada de claves criptográficas son algunos de los problemas más recurrentes.

El objetivo principal de este estudio es evaluar cómo las organizaciones están implementando y auditando los controles de cifrado, con el fin de identificar deficiencias y proponer recomendaciones para mejorar la seguridad y la conformidad con las normativas de protección de datos.

METODOLOGÍA

El estudio se desarrolló bajo un enfoque cuantitativo, dado que se fundamentó en la recolección y análisis de datos numéricos con el objetivo de describir la situación actual de la auditoría de controles de cifrado y protección de la información en los sectores financieros, salud, tecnológico y comercio electrónico.

El tipo de investigación fue descriptivo, ya que se enfocó en caracterizar el estado de adopción, los beneficios percibidos, los desafíos enfrentados y las expectativas futuras en relación con la auditoría de

controles de cifrado y protección de la información.

El diseño de investigación utilizado fue observacional y transversal, dado que los datos se recopilaron en un solo momento del tiempo sin intervenir en las variables analizadas.

La población de estudio estuvo conformada por empresas de la ciudad de Quito, Ecuador, mientras que la muestra se seleccionó mediante un muestreo por conveniencia. Los participantes fueron 36 contadores públicos autorizados que cumplían con los criterios de inclusión establecidos para el estudio.

Para la recolección de datos, se utilizó la técnica de la encuesta, la cual fue aplicada mediante un cuestionario estructurado de 25 ítems. Dicho instrumento fue diseñado para evaluar diferentes aspectos relacionados con la auditoría de controles de cifrado y protección de la información en los sectores financieros, salud, tecnológico y comercio electrónico.

El análisis de los datos obtenidos se llevó a cabo utilizando el software JASP, el cual permitió realizar tanto análisis estadístico como descriptivo, además de facilitar la presentación visual de los resultados mediante gráficos y tablas, contribuyendo así a una mejor interpretación de la información recopilada.

En cuanto a las consideraciones éticas, se aseguró la confidencialidad y anonimato de los participantes, y se obtuvo su consentimiento informado previo a la aplicación del cuestionario.

Los criterios de inclusión consideraron a contadores públicos autorizados con experiencia en auditoría y seguridad de la información dentro de los sectores analizados. En contraste, los criterios de exclusión comprendieron a profesionales que no contaban con experiencia en auditoría o que no estuvieran vinculados con la seguridad de la información.

Finalmente, entre las limitaciones del estudio, se encuentra el uso de un muestreo por conveniencia, lo que podría afectar la generalizabilidad de los resultados. No obstante, los hallazgos proporcionan una base sólida para futuras investigaciones sobre la auditoría de controles de cifrado y protección de la información en los sectores analizados.

RESULTADOS Y DISCUSIÓN

Los datos obtenidos a través de encuestas evidencian tendencias clave en la implementación y auditoría de los controles de cifrado dentro de las organizaciones estudiadas. A continuación, se destacan los principales hallazgos:

Nivel de implementación de cifrado: el 85% de las empresas encuestadas utilizan algún tipo de cifrado

para proteger sus datos, siendo el AES-256 el algoritmo más empleado debido a su robustez y compatibilidad con estándares internacionales de seguridad, como ISO 27001 y NIST 800-53.

Sectores con mayor adopción de cifrado

Sector financiero: el 95% de las empresas han implementado cifrado en sus sistemas para cumplir con normativas estrictas como PCI DSS.

Sector salud: el 75% de las organizaciones protegen la información de pacientes mediante cifrado; sin embargo, solo el 50% realiza auditorías de seguridad de manera periódica.

Sector tecnológico y comercio electrónico: La implementación de cifrado alcanza el 80%, pero más del 40% de las empresas enfrentan problemas con la gestión de claves criptográficas, comprometiendo la seguridad de sus sistemas.

Deficiencias Detectadas

Gestión inadecuada de claves criptográficas: el 70% de las organizaciones carecen de procedimientos claros para la rotación y almacenamiento seguro de claves, aumentando el riesgo de vulnerabilidades.

Falta de capacitación en ciberseguridad: el 55% de los responsables de TI indican que sus empresas no han proporcionado formación específica en auditoría de cifrado, limitando su capacidad para detectar y corregir fallos de seguridad.

Cumplimiento normativo parcial: aunque la mayoría de las empresas han implementado cifrado, solo el 45% cuenta con certificaciones de cumplimiento normativo, lo que podría derivar en sanciones regulatorias en caso de incumplimientos.

Diversos estudios de investigación, como los realizados por Steinbart et al. (2016) y Stafford et al. (2018) han analizado el papel fundamental que juega la auditoría interna en la gestión y gobernanza de riesgos de ciberseguridad. Estos estudios resaltan la importancia de que la auditoría interna se enfoque en evaluar la eficacia del control interno en materia de ciberseguridad. Gale et al., (2022) recopilan datos de estudios relacionados con auditorías de controles de cifrado y protección de la información. Como resultado, Gale et al., (2022) mencionan que las organizaciones están realizando esfuerzos significativos, especialmente en países en desarrollo, para mejorar la ejecución de las auditorías de riesgos de ciberseguridad. Las organizaciones que ya han experimentado problemas de ciberseguridad debido a la falta de auditorías han trabajado en mejorar la competencia de los comités de auditoría

interna e implementar guías prácticas dentro de la organización, definiendo objetivos claros (Gale et al., 2022).

Para ser prácticos, los objetivos relacionados con la auditoría de controles de cifrado y protección de la información, deben ser vistos desde un punto de vista de control interno (Sabillon et al., 2018).

Protección de la Información

La generación, uso, almacenamiento, envío, recuperación y disposición final de la información se fundamenta en procesos y tecnologías que requieren un alto grado de confiabilidad para alcanzar objetivos específicos. Esta necesidad está intrínsecamente ligada a la seguridad de la información, la cual se deriva de buenas prácticas y marcos normativos que sirven como guía.

Al abordar el concepto de seguridad de la información, es evidente que se busca preservar su confidencialidad frente a accesos no autorizados, prevenir alteraciones indebidas que puedan comprometer su integridad y garantizar su disponibilidad. Para ello, la seguridad de la información se apoya en los siguientes principios:

Confidencialidad: Este principio asegura que solo las personas autorizadas tengan acceso a la información, con el propósito de evitar su divulgación sin los permisos necesarios y bajo condiciones específicas.

Integridad: La integridad se refiere a que la información sea precisa, oportuna, completa y coherente. Dado que estas características no pueden ser mantenidas únicamente por sistemas automáticos, se distinguen dos aspectos: la integridad de los datos y la integridad del sistema. La integridad de los datos se centra en la protección de la información y los programas, restringiendo cualquier alteración a personas autorizadas.

Disponibilidad: Este concepto garantiza que la información proporcionada por un sistema sea accesible de manera eficaz y que siempre haya disponibilidad, permitiendo el acceso solo a personas autorizadas.

-Autenticación: Este proceso consiste en identificar a la entidad que genera la información. Al recibir un mensaje, el sistema debe confirmar que proviene del remitente legítimo y no de alguien que haya suplantado su identidad.

No Repudio: Este principio establece que ni el emisor ni el receptor de un mensaje deben poder negar la transmisión del mismo. En otras palabras, el no repudio impide que se rechace la comunicación de

un mensaje por parte del transmisor o del receptor.

El primer principio mencionado ha generado amplias controversias, ya que afecta, entre otros, los derechos humanos fundamentales relacionados con la privacidad y la libertad de expresión, así como diversas cuestiones éticas. Este principio también está estrechamente vinculado a la confianza y al manejo adecuado de la información por parte de los usuarios, quienes son los más vulnerables en los sistemas informáticos. La protección de la intimidad y la confidencialidad de la información se ha convertido en un desafío para los gobiernos, que han enfrentado esta situación mediante varios mecanismos, tales como: educación sobre el ciberespacio y sus riesgos, campañas de concientización sobre la información que no se debe compartir en redes sociales, y la creación de marcos normativos e instituciones que resguardan y protegen la confidencialidad de las comunicaciones y el tratamiento de datos personales.

Seguridad en sistemas

Como se ha mencionado anteriormente, las medidas para garantizar la seguridad en el ciberespacio son tanto preventivas como reactivas. Por un lado, es crucial estar preparado ante posibles ataques y evitar descuidos que puedan comprometer dicha preparación, así como atender las amenazas que surgen a diario. En el ámbito de la prevención, distintas entidades han desarrollado esquemas que orientan a los sectores involucrados en la evaluación de riesgos y el análisis de amenazas y vulnerabilidades, con el objetivo de establecer un entorno seguro para sus sistemas.

Por otro lado, el avance tecnológico frecuentemente exige actualizaciones en los servicios de seguridad implementados, e incluso da lugar a la creación de nuevos servicios. Dado que las políticas abarcan un enfoque general, las organizaciones deben establecer estándares y programas que proporcionen claridad en la ejecución de las soluciones de seguridad. Para ofrecer estos servicios, se han creado los CERT, grupos de especialistas en tecnología que proporcionan respuesta y gestión de seguridad frente a problemas cibernéticos en dispositivos y herramientas tecnológicas, conocidos también como equipos de Respuesta a Incidentes Informáticos. El origen de los CERT se remonta a la década de 1980, surgido a raíz de la propagación del gusano Morris en diversos sistemas a nivel global.

Infraestructura crítica

El término infraestructura crítica se refiere al conjunto de activos tecnológicos esenciales que interactúan

entre sí para ofrecer servicios fundamentales a la población. Estos activos pueden incluir tanto instalaciones físicas como virtuales, redes de datos, redes industriales, sistemas de información, bases de datos, sistemas de control industrial, procesos automatizados, así como cualquier componente tecnológico que facilite la provisión o supervisión de un servicio esencial que beneficie al bien común. Es importante reconocer que estos activos son vulnerables a incidentes de ciberseguridad, dado el elevado número de amenazas presentes en el ciberespacio. Un incidente de este tipo puede impactar diversos sectores de un país, como el sistema de salud, la administración pública, el sector financiero, las telecomunicaciones o los proveedores de energía, entre otros. En este sentido, es crucial considerar que los servicios vitales de un país dependen de infraestructuras críticas, las cuales están compuestas por activos que requieren de protección adecuada

Los hallazgos del estudio confirman que, aunque el cifrado de datos es ampliamente utilizado en las organizaciones, persisten importantes deficiencias en su implementación y auditoría. La falta de procedimientos adecuados para la gestión de claves criptográficas y la ausencia de auditorías continuas son factores clave que incrementan el riesgo de vulnerabilidades en los sistemas de información. Además, la falta de capacitación especializada en auditoría de cifrado contribuye a que las organizaciones no puedan detectar o corregir fallos en sus controles de seguridad.

Comparado con estudios previos, estos resultados refuerzan la idea de que el cifrado, por sí solo, no es suficiente para proteger la información sensible. La gestión adecuada de claves, la realización de auditorías regulares y la formación continua del personal son elementos esenciales para asegurar la efectividad de los controles de cifrado.

ILUSTRACIONES, TABLAS, FIGURAS.

Para facilitar la comprensión y el análisis de los hallazgos y recomendaciones, se han detallado las observaciones, riesgos identificados y medidas a implementar en organizaciones de los sectores financiero, salud, tecnológico y comercio electrónico; en las siguientes tablas:

Tabla 1: Observaciones, riesgos y recomendaciones sobre el estudio realizado

Observación	Riesgo	Recomendación
No se documentan políticas de seguridad de la información.	En caso de negligencia, no existe respaldo documental que demuestre el cumplimiento de las políticas.	Elaborar un documento formal que detalle las políticas y procedimientos de seguridad de la información, aprobado por la alta dirección y revisado regularmente para su actualización periódica.
No se asignan responsables de seguridad de la información en los departamentos de sistemas.	Pueden ocurrir errores graves y fraudes debido a la falta de supervisión en el manejo de la información.	Asignar un responsable capacitado en seguridad de la información, con conocimientos en ISO 27002.
Los empleados no reciben capacitación adecuada sobre seguridad de la información.	El personal puede tomar decisiones incorrectas debido a falta de actualización en políticas de seguridad.	Organizar capacitaciones periódicas sobre actualizaciones en políticas y procedimientos organizacionales.

Nota. Los datos fueron tomados de la encuesta aplicada en la provincia de Pichincha, ciudad de Quito, empresas de los sectores financiero, salud, tecnológico y comercio electrónico

Tabla 2: Identificación de riesgos y amenazas – Cifrado

Observación	Descripción	Riesgo
Cifrado	No se ha desarrollado e implementado una política que regule el uso de controles criptográficos (cifrado) para la protección de la información.	Incumplimiento de normativas y exposición de datos sensibles a ataques externos.

Nota. Los datos fueron tomados de la encuesta aplicada en la provincia de Pichincha, ciudad de Quito, empresas de los sectores financiero, salud, tecnológico y comercio electrónico

CONCLUSIONES

Deficiencias en la gestión de accesos y control de seguridad

Los resultados del análisis revelan la inexistencia de responsables de la seguridad de la información (SI), así como la ausencia de un protocolo de gestión de accesos a los sistemas informáticos. La falta de estos mecanismos incrementa la probabilidad de incidentes de seguridad y dificulta la supervisión efectiva de

los controles de protección de datos. Ante esta situación, se recomienda la asignación de un responsable con conocimientos en normativas como la ISO 27002, con el fin de garantizar la vigilancia y mejora continua de los controles de seguridad implementados.

Capacitación insuficiente en seguridad de la información

Se ha identificado que la capacitación de los empleados en materia de seguridad informática es insuficiente, lo que limita su capacidad para responder de manera adecuada ante incidentes y afecta la implementación efectiva de las políticas de protección de la información. Para abordar esta deficiencia, resulta fundamental diseñar e implementar un programa de formación continua, permitiendo que el personal se mantenga actualizado respecto a las políticas y procedimientos de seguridad establecidos.

Propuestas de investigación futura

El estudio deja abiertos diversos interrogantes relacionados con la implementación efectiva de controles de seguridad en sistemas externos, como el programa SINET que es utilizado en el departamento contable. Se sugiere que futuras investigaciones profundicen en el análisis de sistemas externalizados y su alineación con las políticas internas de seguridad, considerando el papel crucial que estos sistemas desempeñan en la protección de la información financiera.

REFERENCIAS BIBLIOGRÁFICAS

Zuñiga-Paredes, Andrea Raquel, Jalón Arias, Edmundo José, Andrade Olmedo, María Ernestina, & Giler Chango, José Leonardo. (2021). Análisis de seguridad informática en entornos virtuales de la Universidad regional autónoma de los Andes extensión Quevedo en tiempos de covid-19 [Analysis of computer security in virtual environments of the Autonomous regional University of the Andes extension Quevedo in times of covid-19].Revista Universidad y Sociedad,13(3), 454-459.

Coronel-Suárez, I., & Quirumbay-Yagual, D. (2022). Seguridad informática, metodologías, estándares y marco de gestión en un enfoque hacia las aplicaciones web [IT security, methodologies, standards and management framework in a web application approach].Revista Científica Y Tecnológica UPSE,9(2), 97-108. https://doi.org/10.26423/rctu.v9i2.672

Flores-Álava, S., & Mena-Hernández, L. (2023). Propuesta de Buenas Prácticas para Mitigar

Ciberataques en Usuarios de Entidades Financieras [Proposal for Good Practices to Mitigate Cyber-attacks on Users of Financial Institutions].593 Digital Publisher CEIT,8(4), 159-173. https://doi.org/10.33386/593dp.2023.4.1652

Ojeda-Contreras, F., Moreno-Narváez, V., & Torres-Palacios, M. (2020). Gestión del riesgo y la ciberseguridad en el sector financiero popular y solidario del Ecuador [Risk management and cybersecurity in Ecuador's popular and solidarity-based financial sector].CIENCIAMATRIA,6(2), 192-219. https://doi.org/10.35381/cm.v6i2.366