SAN IGNACIO DE LOYOLA – ESCUELA ISIL

TÍTULO DE LA INVESTIGACIÓN

“Propuesta de diseño de políticas de seguridad de la información en el estudio contable JC TICONA”

TRABAJO DE INVESTIGACIÓN PARA OPTAR EL GRADO ACADÉMICO DE

Bachiller en Dirección de Tecnologías de la Información

PRESENTADO POR:

Luna Cutipa, Sergio Juan - Tecnologías de la información

ASESOR:

Sam Anlas, Carlos Antonio

LIMA, PERÚ

2025

ASESOR Y MIEMBROS DEL JURADO

ASESOR:

Sam Anlas, Carlos Antonio

MIEMBROS DEL JURADO

Rojas Aguilar, Claudio Sergio

Espinoza Rua, Celes Alonso

Cosme Raymundo, Tania Adriana

DECLARACIÓN JURADA DE ORIGINALIDAD

Yo, Sergio Juan Luna Cutipa, identificado con DNI N° 46315949 perteneciente al Programa de Dirección de Tecnologías de la Información, siendo mi asesor el Sr Carlos Antonio Sam Anlas, identificado con DNI N° 40789757, y cuyo código ORCID es 0000-0003-1632-7131.

DECLARO BAJO JURAMENTO QUE:

a) Soy el autor del documento académico titulado “Propuesta de diseño de políticas de seguridad de la información en el estudio contable JC TICONA“

b) El trabajo de investigación es original y no ha sido difundido en ningún medio académico; por lo tanto, sus resultados son veraces y no es copia de ningún otro.

c) El trabajo de investigación cumplió con el análisis del sistema TURNITIN, el cual tiene el 19 % de similitud. Se ha respetado el uso de las normas internacionales en cuanto a citas y referencias.

d) Declaro conocer las consecuencias legales y/o administrativas que puedan derivar si se verifica la falsedad total o parcial de la presente declaración, de acuerdo con lo previsto en el artículo 411 del código penal y el numeral 34.3 del artículo 34 del Texto Único Ordenado de la Ley del Procedimiento Administrativo General, aprobado por Decreto Supremo 004-2019-JUS y los artículos 14º y 15º de la RVM 049-2022-MINEDU.

Fecha: 17, diciembre, 2025

Firma del autor

Firma del asesor

ÍNDICE TEMÁTICO

ÍNDICE DE TABLA

ÍNDICE DE GRÁFICOS

RESUMEN

El presente proyecto se desarrolla ante la ausencia de políticas formales de seguridad de la información en el Estudio Contable JC TICONA, situación que genera vulnerabilidades en la confidencialidad de los datos contables y tributarios que gestiona la organización. El objetivo es formular lineamientos conceptuales para el futuro diseño de políticas de seguridad de la información, basados en la norma internacional ISO/IEC 27001:2022, con el fin de establecer directrices normativas y operativas que fortalezcan la gestión de los activos de información y aseguren la continuidad de las operaciones.

El estudio es de tipo aplicado, con enfoque cuantitativo, nivel descriptivo–diagnóstico y diseño no experimental de corte transversal. La unidad de análisis corresponde a los procesos, documentos y controles internos relacionados con la seguridad de la información. La recolección de datos se realizó mediante una lista de cotejo estructurada en tres dominios alineados a la ISO/IEC 27001:2022. El análisis se efectuó a través de una valoración porcentual del nivel de cumplimiento de cada control, clasificando los resultados en tres categorías: Cumple (C), Parcialmente cumple (PC) y No cumple (NC).

Los resultados del diagnóstico muestran que el 88.9 % de los controles se encuentran en condición de cumplimiento parcial, lo que evidencia que la mayoría de los procesos se ejecutan de forma empírica, sin documentos, procedimientos ni lineamientos formales. Asimismo, el 11.1 % de los controles presentan un nivel de incumplimiento crítico, especialmente en aspectos como la clasificación de la información y el inventario de activos, donde no existe evidencia de prácticas implementadas. Con base en estos hallazgos, se formularon lineamientos conceptuales y una ruta referencial para el futuro diseño e implementación de políticas formales de seguridad de la información, abarcando áreas como control de accesos, respaldo y almacenamiento, uso aceptable de la información y respuesta ante incidentes. La pertinencia de la propuesta fue corroborada mediante validación de expertos en seguridad de la información.

Palabras clave: seguridad de la información, ISO/IEC 27001:2022, políticas de seguridad, gestión de riesgos, activos de información.

ABSTRACT

This project was developed in response to the absence of formal information security policies at the JC TICONA Accounting Firm, a situation that creates vulnerabilities in the confidentiality of the accounting and tax data managed by the organization. The objective is to formulate conceptual guidelines for the future design of information security policies based on the international standard ISO/IEC 27001:2022, in order to establish regulatory and operational directives that strengthen the management of information assets and ensure the continuity of organizational operations.

The study is applied in nature, with a quantitative approach, a descriptive–diagnostic level, and a non-experimental cross-sectional design. The unit of analysis corresponds to the processes, documents, and internal controls related to information security. Data collection was carried out through a structured checklist organized into three domains aligned with ISO/IEC 27001:2022. The analysis was conducted through a percentage-based assessment of the level of compliance for each control, classifying the results into three categories: Compliant (C), Partially Compliant (PC), and Non-Compliant (NC).

The diagnostic results show that 88.9% of the controls are in a condition of partial compliance, indicating that most processes are carried out empirically, without formal documents, procedures, or guidelines. In addition, 11.1% of the controls present a critical level of non-compliance, particularly in areas such as information classification and asset inventory, where there is no evidence of implemented practices. Based on these findings, conceptual guidelines and a reference roadmap were formulated for the future design and implementation of formal information security policies, covering areas such as access control, backup and storage management, acceptable use of information, and incident response. The relevance of the proposal was confirmed through validation by experts in information security.

Keywords: information security, ISO/IEC 27001:2022, security policies, risk management, information assets.

INTRODUCCIÓN

La gestión adecuada de la seguridad de la información se ha convertido en un requisito esencial para las organizaciones que manejan datos sensibles, especialmente en el sector contable, donde la integridad, confidencialidad y disponibilidad de la información son fundamentales para garantizar la continuidad operativa y el cumplimiento normativo. En este contexto, el estudio contable JC TICONA enfrenta un problema crítico: la ausencia de políticas formales de seguridad de la información. Esta carencia expone a la organización a riesgos significativos, como pérdida o alteración de datos, accesos no autorizados, fallas en los respaldos y vulnerabilidades en los procesos de almacenamiento y uso de información contable y tributaria.

Las prácticas actuales se basan en procedimientos informales y no estandarizados, lo cual limita la eficacia de los mecanismos de protección y dificulta la capacidad de respuesta ante incidentes. Esta situación evidencia la necesidad de implementar lineamientos claros, estructurados y alineados a estándares internacionales que permitan elevar el nivel de madurez digital del estudio y fortalecer la protección de sus activos de información.

La norma ISO/IEC 27001:2022 constituye un marco reconocido globalmente para la gestión de la seguridad de la información, proporcionando requisitos y controles que permiten establecer políticas, procedimientos y prácticas operativas robustas. Su aplicación resulta pertinente para organizaciones que buscan consolidar un sistema de gestión de seguridad adaptable, eficiente y verificable.

El propósito de este proyecto es plantear y sustentar la necesidad de contar con políticas de seguridad de la información alineadas con dicho marco. Para ello, se realiza un diagnóstico del nivel de cumplimiento mediante una lista de cotejo estructurada en dominios clave, lo que permite identificar brechas, riesgos y áreas críticas que requieren intervención inmediata. A partir de estos resultados, se justifica la elaboración futura de

políticas formales, evidenciando por qué el estudio necesita fortalecer la protección de sus datos contables y tributarios.

Finalmente, el proyecto aporta una base metodológica y analítica que orienta a la organización hacia la formalización de sus procesos de seguridad, contribuyendo a mejorar la continuidad operativa, definir criterios de uso y acceso a la información y promover una cultura organizacional orientada a la ciberseguridad. En consecuencia, este trabajo constituye una herramienta útil para elevar la confiabilidad, eficiencia y resiliencia del estudio contable JC TICONA frente a los riesgos tecnológicos actuales.

1. INFORMACIÓN GENERAL

1.1. Título del Proyecto

Propuesta de diseño de políticas de seguridad de la información en el estudio contable JC TICONA.

1.2. Área estratégica de desarrollo prioritario

La línea de investigación de ISIL en Aplicaciones Tecnológicas y Transformación Digital se enfoca en desarrollar procesos mediante el uso de tecnologías innovadoras, generando soluciones específicas y modelos predictivos para la toma de decisiones y fomentando la incorporación de tecnología en todos los procesos de valor.

En el contexto del estudio contable JC TICONA, la investigación no solo persigue la protección de los activos de información, sino también optimizar la eficiencia operativa, garantizar la continuidad de los servicios y salvaguardar la integridad de la información. Todo esto se lleva a cabo en concordancia con las necesidades y exigencias del entorno digital actual, promoviendo así un enfoque integral de seguridad que favorece el desarrollo sostenible y la competitividad de la organización.

1.3. Actividad económica en la que se aplicaría la investigación

La actividad económica en la que se desarrollará esta investigación corresponde al sector de servicios contables y financieros, específicamente en el estudio contable JC TICONA. Este sector maneja información altamente sensible como estados financieros, declaraciones tributarias y registros laborales por lo que la seguridad de la información es esencial para garantizar la continuidad operativa y la confianza de los clientes.

El informe *La Ciberdelincuencia en el Perú: Estrategias y Retos del Estado* evidencia un incremento sostenido de los ciberdelitos en el país, siendo el fraude informático y la suplantación de identidad los más recurrentes, concentrando juntos más del 90 % de las denuncias registradas (Defensoría del Pueblo, 2022). Esta situación refleja un entorno digital de alto riesgo para las organizaciones que no cuentan con medidas adecuadas de protección. En este contexto, la presente propuesta busca fortalecer la seguridad de la

información, reducir vulnerabilidades internas, desarrollar competencias digitales en el personal y asegurar la continuidad operativa frente a amenazas cibernéticas.

1.4. Alcance de la solución

El alcance de la solución propuesta consiste en establecer lineamientos conceptuales para el futuro diseño de políticas de seguridad de la información en el estudio contable JC TICONA, tomando como referencia la norma ISO/IEC 27001:2022. Estos lineamientos se formulan a partir de los resultados del diagnóstico realizado y permiten definir los componentes mínimos que deberán considerar las futuras políticas formales del estudio.

2. DESCRIPCION DE LA INVESTIGACION APLICADA

2.1. Formulación del problema

2.1.1. Problema general

¿Qué elementos deben identificarse para formular lineamientos conceptuales para el futuro diseño de políticas de seguridad de la información alineadas con la norma ISO/IEC 27001:2022 en el estudio contable JC TICONA?

2.1.2. Problemas específicos

P1: ¿Qué políticas, normas o procedimientos relacionados con el acceso, uso y almacenamiento de información confidencial existen actualmente en el estudio contable JC TICONA?

P2: ¿Qué riesgos y vulnerabilidades se identifican en el estudio contable JC TICONA debido a la ausencia o insuficiencia de políticas de seguridad de la información?

P3: ¿Qué lineamientos mínimos deben considerarse para formular lineamientos conceptuales para el futuro diseño de políticas de seguridad de la información acordes con la realidad organizacional del estudio contable JC TICONA?

2.2. Objetivos de investigación

2.2.1. Objetivo general

Formular lineamientos conceptuales y una ruta referencial para el futuro diseño de políticas de seguridad de la información alineadas con la ISO/IEC 27001:2022 para el Estudio Contable JC TICONA.

2.2.2. Objetivos específicos

OE1: Identificar las políticas, normas o procedimientos existentes relacionados con el acceso, uso y almacenamiento de información confidencial en el estudio contable JC TICONA.

OE2: Describir los riesgos y vulnerabilidades presentes debido a la ausencia o insuficiencia de políticas de seguridad de la información.

OE3: Determinar los lineamientos mínimos necesarios para el diseño de políticas de seguridad de la información adaptadas a la realidad del estudio contable JC TICONA.

2.3. Justificación de la investigación

2.3.1. Justificación teórica

La investigación se fundamenta en los principios de la ISO/IEC 27001:2022, un marco reconocido internacionalmente para la gestión de la seguridad de la información. En este estudio, la norma se utiliza como referencia conceptual para el diseño de políticas, sin abordar la implementación de un Sistema de Gestión de la Seguridad de la Información (SGSI). Se consideran conceptos clave como activos de información, análisis de riesgos, control de accesos y mejora continua para estructurar normas internas que guíen el manejo seguro de la información. Dado que el estudio contable JC TICONA gestiona datos financieros, tributarios y contables, es pertinente adaptar estos principios a un entorno con recursos limitados, propio de una microempresa contable en el Perú.

2.3.2. Justificación metodológica

El proyecto adopta un enfoque aplicado, descriptivo–diagnóstico y propositivo. La norma internacional se toma como guía metodológica para realizar un levantamiento de información, identificar activos críticos, valorar riesgos y, con base en ello, formular lineamientos conceptuales para el futuro diseño de políticas de seguridad acordes al contexto del estudio contable JC TICONA. Este enfoque garantiza validez técnica y viabilidad operativa sin requerir herramientas costosas ni equipos especializados. El uso de listas de cotejo y análisis estructurado de brechas permite que los resultados sean directamente aplicables como insumo normativo, lo cual facilitará una implementación gradual si la organización lo decide.

2.3.3. Justificación práctica

El estudio contable JC TICONA carece de políticas formales y procedimientos documentados para proteger su información, lo que incrementa el riesgo de pérdidas de datos, accesos no autorizados e interrupciones operativas. Frente a este escenario, la

propuesta establece un conjunto de lineamientos conceptuales orientados a abordar aspectos críticos como el control de accesos, el uso aceptable de la información, el respaldo y recuperación de datos y la gestión inicial de incidentes. Estos lineamientos constituyen una base estructurada para el futuro diseño del manual de políticas de seguridad de la información, fortaleciendo la continuidad operativa y reduciendo la exposición a riesgos, sin requerir infraestructura compleja ni la implementación inmediata de un SGSI.

3. MARCO REFERENCIAL

3.1. Antecedentes de la investigación

3.1.1. Antecedentes nacionales

En su tesis ISO 27001 para mejorar la seguridad de la información en una institución educativa, Lima 2022, Asqui Zevallos y Torres Vásquez (2023) implementaron controles del Anexo A de la ISO 27001 y evaluaron su impacto en los indicadores de confidencialidad, integridad y disponibilidad. Los resultados mostraron una reducción significativa de incidentes: 61.38 % en confidencialidad, 61.73 % en integridad y 61.83 % en disponibilidad, demostrando la eficacia del SGSI para fortalecer los activos informacionales de una institución educativa. Los autores concluyen que la norma contribuye directamente a mejorar la seguridad de la información mediante políticas y controles formales.

Contador Minaya y Tapia Huamán (2024), en la investigación Diseño e implementación de la ISO 27001 para mejorar la seguridad de información de la Empresa Minera Colibrí S.A.C., analizaron la influencia del diseño e implementación del SGSI en equipos de red, software y hardware de la empresa minera. Identificaron riesgos vinculados al uso de equipos no certificados, ausencia de licencias originales y vulnerabilidades operativas. Tras aplicar instrumentos de evaluación y validación ($\alpha = 0.82$), concluyeron que la ISO 27001 mejora de manera significativa la gestión de la seguridad de la información, fortaleciendo la protección de datos y la infraestructura tecnológica.

Ticona Llerena (2021), en su tesis Uso de la norma ISO 27001 y su influencia en la seguridad de información de la empresa ICO, desarrolló un estudio preexperimental mediante pretest–postest aplicado a 18 unidades de análisis. El autor evaluó las dimensiones de confidencialidad, integridad, disponibilidad y riesgos, aplicando un cuestionario estructurado. Los resultados evidenciaron mejoras significativas en todas las dimensiones tras la aplicación del SGSI, confirmando que la ISO 27001 contribuye a fortalecer la seguridad de la información en organizaciones peruanas a través de controles y políticas formales.

3.1.2. Antecedentes internacionales

Guarneros Moreno (2023), en su investigación *Implementación de políticas de seguridad de información basados en ISO 27001*, desarrolló un conjunto estructurado de políticas alineadas al estándar ISO/IEC 27001 para el departamento de Servicios Educativos de una institución tecnológica en México. El autor identificó activos críticos, evaluó amenazas mediante MAGERIT y aplicó herramientas como PILAR para valorar riesgos. La implementación propuesta incluyó políticas de seguridad operativa, controles de continuidad del negocio, gestión de incidentes y capacitación del personal. El estudio concluye que la adopción sistemática de políticas basadas en ISO 27001 incrementa la confiabilidad, integridad y disponibilidad de la información, fortaleciendo la madurez del SGSI institucional.

Lagos Melo (2024), en su tesis doctoral *Transformación digital y ciberseguridad*, analizó la relación entre la transformación digital, la gestión de la ciberseguridad y las capacidades dinámicas organizacionales. Mediante un enfoque mixto —análisis bibliométrico, entrevistas a CISOs y un modelo SEM— el estudio evidenció que la transformación digital incrementa la exposición a amenazas, pero también impulsa la resiliencia organizacional cuando se aplican marcos de seguridad como el NIST CSF. Asimismo, los hallazgos revelaron que la ambidiestralidad en ciberseguridad (equilibrio entre innovación y protección) tiene un impacto significativo en el rendimiento de la seguridad y la preparación

ante incidentes. El autor concluyó que las organizaciones requieren integrar gobernanza, cultura de seguridad y capacidades adaptativas para sostener su seguridad en entornos digitales complejos.

Ortiz Buitrón (2021), en su trabajo *Diseño de las políticas de seguridad de la información en la Compañía de Seguros S.A.*, desarrolló un conjunto de políticas alineadas a la ISO/IEC 27001:2013 para una entidad aseguradora en Colombia. El estudio identificó activos críticos, analizó vulnerabilidades y evaluó riesgos inherentes y residuales, evidenciando brechas significativas en políticas existentes. La autora destacó que el incremento de la ciberdelincuencia tras la pandemia exige lineamientos claros, controles robustos y cumplimiento regulatorio (Circular 029/2014 y 033/2020). Se concluyó que el diseño e implementación de políticas basadas en ISO 27001 mejora la gestión del riesgo, fortalece la cultura de seguridad y protege la información de clientes, colaboradores y operaciones críticas.

3.2. Marco teórico

Políticas de seguridad de la información

Las políticas de seguridad de la información son un conjunto de normas internas que establecen las reglas, procedimientos y buenas prácticas que debe seguir una organización para proteger sus datos frente a amenazas internas y externas, garantizando así la continuidad de sus actividades. Estas políticas deben contemplar todos los activos que procesan información —como sistemas, servidores, redes, dispositivos móviles y bases de datos—, además de definir mecanismos de control, monitoreo, acceso, respaldo, tratamiento de incidentes, clasificación de la información y uso responsable de los recursos. El Informe de Madurez Digital en las Empresas Peruanas (Ministerio de la Producción, 2023) advierte que gran parte de las empresas del país aún no cuenta con políticas formalizadas de seguridad de la información. En concreto, el 67 % no dispone de un catálogo actualizado de activos digitales, lo que dificulta el establecimiento de políticas adecuadas. Este vacío normativo incrementa la vulnerabilidad frente a amenazas

informáticas y limita la capacidad de respuesta ante incidentes. Por tanto, la elaboración de políticas debe basarse en el conocimiento de los activos tecnológicos y en un análisis de riesgos que permita definir responsabilidades claras, acciones preventivas y protocolos de actuación.

Incidentes informáticos

El Informe “La Ciberdelincuencia en el Perú” (Defensoría del Pueblo, 2023) identifica diversos tipos de fallos y ataques informáticos ocurridos en el país, vinculados directamente con delitos cibernéticos como el acceso ilícito, la interceptación de comunicaciones, la alteración de datos y el sabotaje informático. Dichos incidentes vulneran derechos fundamentales como la privacidad, la propiedad y la seguridad ciudadana, afectando tanto a instituciones públicas como privadas.

El documento también advierte que la capacidad del Estado peruano para prevenir y sancionar estos actos sigue siendo limitada, lo cual resalta la necesidad de una política nacional de seguridad de la información sólida e integrada con capacidades técnicas de monitoreo, respuesta e investigación.

Protección de la información

La *Guía de Protección de Datos por Defecto* (AEPD, 2020) establece que la protección de la información debe integrarse desde la fase de diseño de cualquier sistema o tratamiento de datos, garantizando por defecto que solo se recopile, procese y conserve la información estrictamente necesaria. Este enfoque exige aplicar medidas técnicas y organizativas que limiten la cantidad de datos tratados, su accesibilidad y su tiempo de conservación, evitando que terceros no autorizados puedan acceder a la información sin intervención del titular.

La guía también resalta que la seguridad debe incorporarse automáticamente en todos los sistemas y procesos donde se manejen datos personales, estableciendo controles que reduzcan la exposición, el impacto y el riesgo de accesos indebidos o usos no previstos. Esta aproximación, sustentada en los principios del RGPD, refuerza la responsabilidad

proactiva de las organizaciones y promueve un tratamiento respetuoso, seguro y proporcional de la información, asegurando su confidencialidad, integridad y disponibilidad.

Norma ISO/IEC 27001

La Norma ISO/IEC 27001:2022, *Seguridad de la información, ciberseguridad y protección de la privacidad — Sistemas de gestión de la seguridad de la información — Requisitos*, define los criterios para establecer, operar y mejorar un Sistema de Gestión de la Seguridad de la Información (SGSI). Esta norma forma parte de la familia 27000, originada como la norma británica BS 7799 en 1995 y desarrollada conjuntamente por la Organización Internacional de Normalización (ISO) y la Comisión Electrotécnica Internacional (IEC).

Políticas de seguridad

Desde la perspectiva del CCN-STIC 801 – Responsabilidades, una política de seguridad de la información constituye el instrumento normativo fundamental que orienta la gestión institucional en materia de protección de datos y activos digitales. Este documento oficial señala que la política debe ser aprobada por la alta dirección y difundida de manera formal, garantizando que cada rol dentro de la organización comprenda las obligaciones y responsabilidades que le competen, particularmente en relación con la gestión de riesgos, la implementación de controles y el aseguramiento del cumplimiento normativo. Asimismo, se enfatiza que la política debe mantener coherencia interna, actualizarse periódicamente y permanecer accesible para toda la entidad, de modo que facilite una gobernanza clara, una estructura de responsabilidades bien definida y el desarrollo de una cultura organizacional orientada a la seguridad de la información.

3.2.1. Definición de términos básicos

ISO/IEC 27001:2022

Estándar internacional que determina los requisitos para implementar, mantener y mejorar un Sistema de Gestión de la Seguridad de la Información (SGSI), con el propósito de proteger la confidencialidad, integridad y disponibilidad de los datos mediante controles técnicos y organizativos (ISO/IEC, 2022).

ISO/IEC 27002:2022

Estándar internacional que proporciona un conjunto de controles, directrices y buenas prácticas para implementar medidas de seguridad de la información dentro de una organización. Sirve como referencia complementaria a la ISO/IEC 27001:2022, detallando cómo aplicar y fortalecer los controles de seguridad para proteger la confidencialidad, integridad y disponibilidad de la información en el SGSI (ISO/IEC, 2022).

Sistema de Gestión de Seguridad de la Información (SGSI)

Un SGSI es un marco estructurado que permite gestionar la seguridad de la información de forma sistemática y continua. Se basa en el ciclo PDCA (Planificar, Hacer, Verificar, Actuar) y se implementa para minimizar riesgos y cumplir con las políticas de seguridad establecidas. (ISO/IEC, 2022).

Confidencialidad

Principio fundamental de la seguridad de la información que garantiza que los datos sean accesibles sólo para personas autorizadas. Su objetivo es proteger la información sensible frente a accesos no autorizados o divulgación indebida (ISO/IEC, 2022).

Integridad de la información

Calidad que asegura que los datos permanezcan exactos, completos y no hayan sido modificados sin autorización durante su procesamiento o almacenamiento. Es un pilar esencial junto a la confidencialidad y disponibilidad (NIST, 2023).

Política de seguridad de la información

Conjunto de normas y directrices internas que establecen las reglas de comportamiento y las responsabilidades del personal en el manejo de los activos de información. Constituye la base del marco de control del SGSI (Ministerio de la Producción, 2023).

Riesgo informático

Probabilidad de que una amenaza aproveche una vulnerabilidad y cause un impacto negativo sobre los activos de información o los procesos críticos de la organización. Se evalúa mediante análisis de impacto y probabilidad (ISO/IEC 27005, 2022).

Incidente de seguridad

Evento inesperado o indeseado que compromete la confidencialidad, integridad o disponibilidad de la información. Incluye ataques informáticos, accesos no autorizados, pérdida de datos o fallos en los sistemas (Defensoría del Pueblo, 2023).

Autenticación

Proceso mediante el cual un sistema verifica la identidad de un usuario o entidad antes de conceder acceso a los recursos o servicios. La autenticación puede realizarse mediante contraseñas, certificados digitales, biometría u otros factores combinados en sistemas multifactor (NIST, 2023).

Control de acceso

Conjunto de mecanismos y políticas diseñadas para restringir el acceso a la información solo a usuarios autorizados, basándose en roles, privilegios o identidades verificadas. Su aplicación protege los datos de accesos no autorizados o manipulaciones indebidas (ISO/IEC 27002, 2022).

Activo de información

Todo elemento que posee valor para la organización y que requiere protección, incluyendo datos, equipos, software, documentación, personal y reputación corporativa. La gestión de activos de información es el primer paso en la implementación de un SGSI (ISO/IEC 27001, 2022).

4. METODOLOGÍA DE LA INVESTIGACIÓN

4.1. Diseño metodológico

El proyecto adopta un enfoque cuantitativo, con un alcance descriptivo-propositivo, orientado a evaluar el nivel de cumplimiento de los requisitos de seguridad de la información establecidos en la norma ISO/IEC 27001:2022 dentro del estudio contable JC TICONA, con fines de identificar brechas y formular lineamientos conceptuales para el futuro diseño de políticas de seguridad de la información alineadas con dicha norma.

El diseño de la investigación es no experimental y transversal, dado que se analizan las condiciones existentes sin manipular variables, observando la situación actual de la organización en un único momento del tiempo.

4.1.1. Unidad de análisis

La unidad de análisis estuvo constituida por las prácticas operativas de los cuatro colaboradores del estudio contable JC TICONA en materia de seguridad de la información, así como por los documentos, procesos, controles y evidencias institucionales asociados a dichas prácticas.

Esto comprende los siguientes elementos:

Documentos y procedimientos internos

- Recepción, validación y archivo de comprobantes electrónicos (facturas, boletas, notas).
- Cálculo y registro de IGV, Renta mensual, percepciones y retenciones.
- Elaboración de PLAME (AFP, SNP, ESSALUD).
- Cálculo de CTS, gratificaciones, vacaciones y beneficios sociales.
- Procesamiento de la planilla electrónica y emisión de constancias.
- Conciliación bancaria y cruce de información con libros contables.

Registros contables

- Libros electrónicos: Libro Diario, Libro Mayor y Libro de Inventarios y Balances.
- Registros de ventas, compras y honorarios electrónicos.

- Declaraciones mensuales y anuales enviadas a SUNAT.
- Reportes financieros internos: estados de resultados, comprobaciones y balances.
- Documentación y reportes asociados a auditorías internas o externas.
- Sustentos electrónicos de detracciones y constancias de depósito.

Controles de acceso

- Gestión de contraseñas en software contable (Concar).
- Perfiles de usuario y restricciones de acceso según rol (auxiliar, asistente, contador senior).
- Control de acceso físico a archivadores, oficinas y equipos (llaves, candados, gabinetes).
- Restricciones sobre el uso de dispositivos externos (USB, discos portátiles).
- Control de acceso a carpetas compartidas, servicios en la nube.
- Procedimientos de alta y baja de cuentas para trabajadores o practicantes.

Evidencias de respaldo (Backups)

- Copias de seguridad de libros electrónicos, declaraciones y reportes mensuales.
- Backups automáticos generados por el software contable.
- Almacenamiento seguro en discos externos, servicios en la nube o servidores internos.
- Procedimientos de recuperación de información ante fallos o pérdidas.
- Respaldos históricos de facturación electrónica (XML).
- Archivo digital de contratos, constancias de detracción y documentación laboral (AFP).

Inventario de activos

- Equipos de cómputo, laptops, impresoras, routers y módems.
- Software contable y de facturación (Concar).
- Bases de datos de clientes, contratos y archivos XML.
- Espacios de almacenamiento virtual (Google Drive y OneDrive).
- Dispositivos móviles que contienen información del estudio.
- Documentos físicos internos o pertenecientes a clientes.

Documentación administrativa

- Contratos de servicios contables.
- Órdenes de trabajo, autorizaciones de acceso y permisos internos.
- Reglamentos internos, procedimientos o manuales operativos vigentes.
- Comunicaciones internas sobre manejo y protección de la información.
- Documentos de cese o desvinculación (entrega de claves, devolución de equipos, cierres de acceso).

4.2. Población

La población de estudio está constituida por cuatro colaboradores del estudio contable JC TICONA, entre los cuales se incluyen el gerente general, el contador jefe y dos asistentes contables. Todos los integrantes de esta población gestionan activos de información críticos, tales como documentos contables, bases de datos, registros tributarios y financieros, participando directamente en los procesos administrativos y operativos evaluados.

4.3. Muestra

Debido a que la población fue reducida, accesible y plenamente identificable, se trabajó con una muestra censal, es decir, la totalidad de los cuatro colaboradores del estudio. Esto permite obtener una visión integral y precisa de las prácticas, vulnerabilidades y necesidades reales de seguridad de la información.

4.4. Técnica e instrumentos de recolección de datos

4.4.1. Técnica de recolección de datos

Se empleó la técnica de observación estructurada, adecuada para examinar el nivel de cumplimiento de controles, documentos y mecanismos de seguridad de la información presentes en la organización.

4.4.2. Instrumento de recolección de datos

El instrumento fue una lista de cotejo, elaborada a partir de los requisitos de la norma ISO/IEC 27001:2022. Esta lista se estructuró en tres dominios vinculados directamente a los problemas específicos:

- **Dominio 1 (P1):** Verificación de políticas, normas o procedimientos para el acceso, almacenamiento y uso de información confidencial.
- **Dominio 2 (P2):** Identificación de riesgos y vulnerabilidades basadas en la ausencia o deficiencia de controles (respaldos, accesos, registros, capacitación).
- **Dominio 3 (P3):** Determinación de lineamientos mínimos necesarios para formular lineamientos conceptuales para el futuro diseño de políticas de seguridad de la información acordes con la realidad organizacional.

Cada ítem del instrumento fue evaluado mediante una escala cualitativa ordinal, conforme al nivel de implementación observado:

- **Cumple (C):** El control está documentado e implementado adecuadamente.
- **Parcialmente cumple (PC):** Existe documentación o práctica informal, pero no estandarizada.

- **No cumple (NC):** No existe evidencia documentada ni práctica implementada.

Esta escala permitió identificar brechas específicas y sustentar la formulación de lineamientos conceptuales para el futuro diseño de políticas de seguridad de la información alineadas con la ISO/IEC 27001:2022.

4.4.3. Validez y confiabilidad del instrumento

Validez: La lista de cotejo fue sometida a juicio de expertos en seguridad de la información, quienes evaluaron la claridad, pertinencia y correspondencia de los ítems con los controles de la norma ISO/IEC 27001:2022. La revisión permitió ajustar la redacción de los ítems y verificar su coherencia con los objetivos específicos del estudio.

Confiabilidad: La confiabilidad del instrumento se aseguró mediante criterio de consistencia de aplicación, a partir de la revisión uniforme de evidencias documentarias y operativas bajo una misma escala de valoración (C, PC y NC). Para ello, se establecieron criterios de observación homogéneos que permitieron mantener estabilidad en la interpretación y registro de los hallazgos.

4.4.4. Procedimiento

- Revisión de los requisitos de la ISO/IEC 27001:2022 y los controles del Anexo A
- Elaboración de la lista de cotejo estructurada por dominios.
- Validación del instrumento mediante juicio de expertos.
- Observación estructurada de evidencias (documentos, procesos y controles del estudio).
- Registro del nivel de cumplimiento mediante la escala C–PC–NC.
- Consolidación de resultados y análisis descriptivo de brechas.

DIMENSIÓN 1: Políticas y procedimientos de seguridad (P1)

Evalúa la existencia, claridad y aplicación de políticas documentadas que regulan el tratamiento de información.

Tabla 1
DIMENSIÓN 1: Políticas y procedimientos de seguridad

Indicadores	Ítems (lista de cotejo)	Escala de valoración
Existencia de políticas documentadas	¿Existe una política general de seguridad de la información aprobada y comunicada?	C – PC – NC
Roles y responsabilidades de seguridad	¿Se han definido roles y responsabilidades de seguridad de la información?	C – PC – NC
Inventario de activos	¿La organización posee un inventario de activos de información actualizado?	C – PC – NC
Uso y protección de la información	¿Se aplican reglas de uso aceptable de la información y los recursos informáticos?	C – PC – NC
Clasificación y etiquetado de la información	¿La información se clasifica y etiqueta según su nivel de confidencialidad? *()*	C – PC – NC
Procedimientos de acceso a la información	¿Existen procedimientos documentados para el control de accesos?	C – PC – NC

DIMENSIÓN 2: Identificación de riesgos y brechas (P2)

Analiza la existencia de mecanismos para detectar, registrar y gestionar riesgos relacionados con la información.

Tabla 2
DIMENSIÓN 2: Identificación de riesgos y brechas

Indicadores	Ítems (lista de cotejo)	Escala de valoración
Identificación de vulnerabilidades	¿La organización realiza análisis o evaluación periódica de riesgos de seguridad de la información?	C – PC – NC
Controles de respaldo	¿Se cuenta con medidas documentadas de respaldo y restauración de la información?	C – PC – NC

Control de accesos	¿Existen controles de acceso físicos y lógicos (roles, permisos, contraseñas seguras)?	C – PC – NC
Protección contra vulnerabilidades	¿Se aplican medidas de protección contra malware y vulnerabilidades técnicas?	C – PC – NC
Registro de incidentes	¿Se dispone de mecanismos de monitoreo o registro de eventos de seguridad?	C – PC – NC
Capacitación en riesgos	¿El personal recibe capacitación y concientización en seguridad de la información?	C – PC – NC

DIMENSIÓN 3: Lineamientos para el diseño de políticas de seguridad (P3)

Evalúa si existen prácticas mínimas para formular políticas adecuadas al contexto organizacional.

Tabla 3
DIMENSIÓN 3: Lineamientos para el diseño de políticas de seguridad

Indicadores	Ítems (lista de cotejo)	Escala de valoración
Procedimientos mínimos establecidos	¿Se planifica la gestión de incidentes de seguridad (detección, respuesta y registro)?	C – PC – NC
Controles esenciales implementados	¿Se prevén acciones para aprender de los incidentes y mejorar controles?	C – PC – NC
Gestión de activos de información	¿Existen medidas para la protección de datos personales y confidenciales?	C – PC – NC
Responsable de seguridad	¿Se incluyen disposiciones sobre uso de dispositivos personales y trabajo remoto?	C – PC – NC
Prácticas de mejora continua	¿Se definen políticas de copia de seguridad y eliminación segura de información?	C – PC – NC
Continuidad operativa	¿Se contempla la continuidad del negocio ante incidentes o interrupciones?	C – PC – NC

Técnica de procesamiento de la información

Análisis descriptivo

DOMINIO 1 – Existencia de políticas y procedimientos (P1)

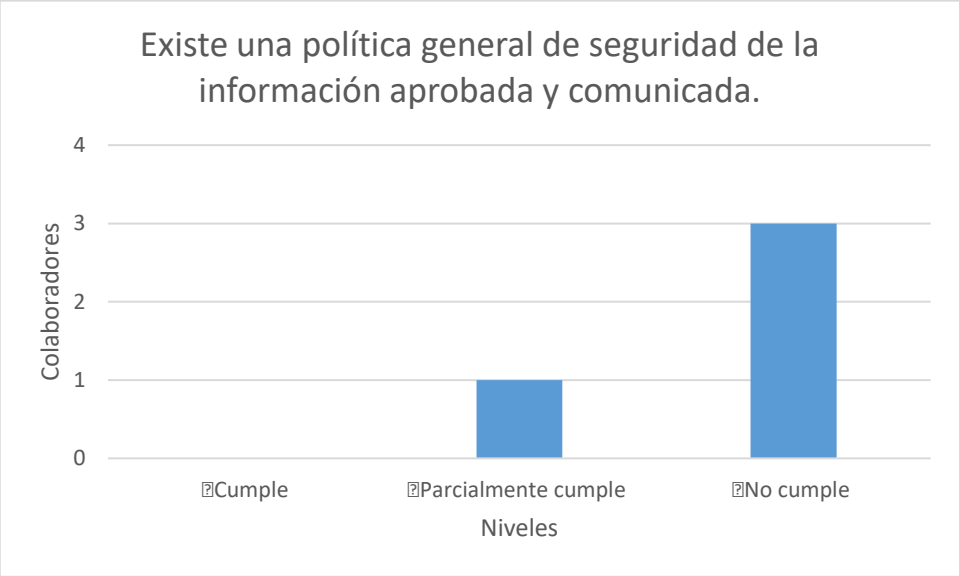
Ítem de evaluación N.º 01

Tabla 4
Existencia de políticas documentadas

Niveles	Existe una **política general de seguridad de la información** aprobada y comunicada.
Cumple	0
Parcialmente cumple	1
No cumple	3
Total general	4

Nota. Elaboración propia

Figura 1
Existencia de políticas documentadas



Nota: En el estudio contable JC TICONA no se cuenta con una política general de seguridad de la información aprobada ni difundida entre el personal. Si bien se aplican medidas básicas de resguardo por hábito o sentido común, no existen lineamientos escritos ni procedimientos normalizados que orienten la gestión segura de los activos de información.

Este hallazgo evidencia la necesidad de diseñar e implementar una política formal de seguridad de la información, conforme a la cláusula 5.1 de la ISO/IEC 27001:2022, que

establezca responsabilidades, mecanismos de comunicación y compromisos de cumplimiento aplicables a todos los colaboradores.

Conclusión: No existe una política formal ni evidencia de aprobación o difusión interna; la gestión de seguridad se basa en prácticas empíricas y criterios personales.

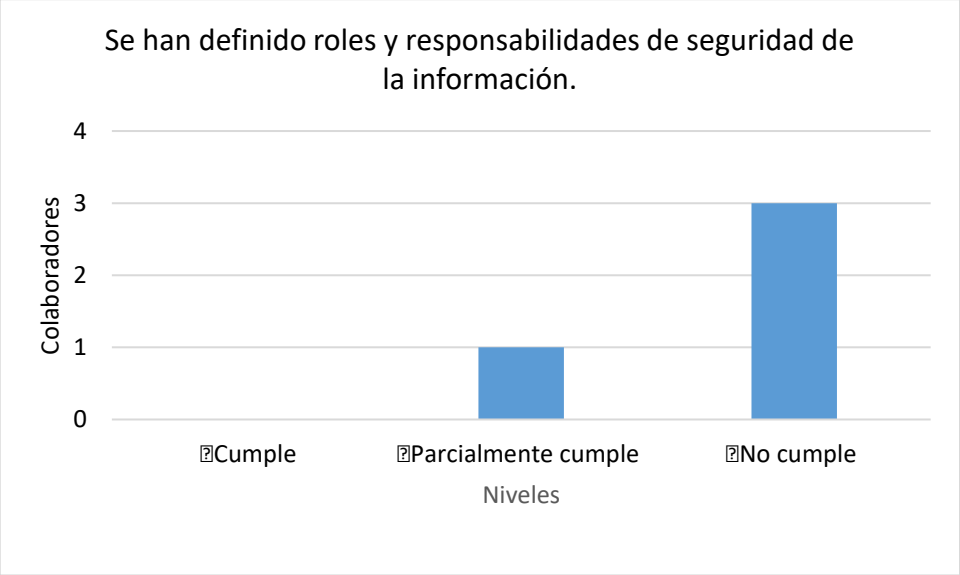
Ítem de evaluación N.º 02

Tabla 5
Roles y responsabilidades de seguridad

Niveles	Se han definido roles y responsabilidades de seguridad de la información.
Cumple	0
Parcialmente cumple	1
No cumple	3
Total general	4

Nota. Elaboración propia

Figura 2
Roles y responsabilidades de seguridad



Nota: En el estudio contable JC TICONA no se han definido formalmente los roles ni las responsabilidades vinculadas a la seguridad de la información. Las funciones relacionadas con la protección de los datos son asumidas de manera empírica, sin asignación específica ni respaldo documental.

Este hallazgo evidencia la necesidad de establecer y comunicar claramente las responsabilidades de cada cargo, conforme a la cláusula 5.2 de la ISO/IEC 27001:2022,

de modo que se asegure la rendición de cuentas y la gestión efectiva de los riesgos.

Conclusión: No existen roles definidos ni documentación que respalde las responsabilidades en materia de seguridad; las acciones se ejecutan de forma informal y sin coordinación estructurada.

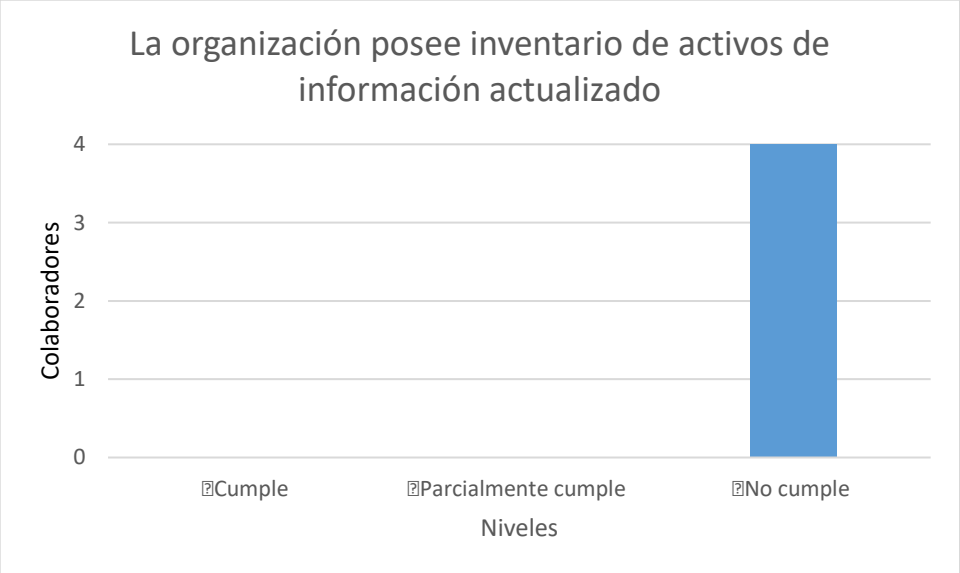
Ítem de evaluación N.º 03

Tabla 6
Inventario de activos

Niveles	La organización posee inventario de activos de información actualizado.
Cumple	0
Parcialmente cumple	0
No cumple	4
Total general	4

Fuente: Elaboración propia

Figura 3
Inventario de activos



Fuente: Elaboración propia

Nota: En el estudio contable JC TICONA no se dispone de un inventario de activos de información formalmente elaborado ni actualizado. Los equipos, archivos y bases de datos son administrados por cada colaborador sin control unificado ni registro de propiedad o ubicación.

Este hallazgo evidencia la necesidad de implementar un inventario documentado de activos, conforme a la cláusula 5.9 de la ISO/IEC 27001:2022, que permita identificar los

recursos de información, sus responsables y el nivel de protección requerido.

Conclusión: No existe un inventario formal de activos de información; la gestión actual se realiza de manera dispersa y sin trazabilidad.

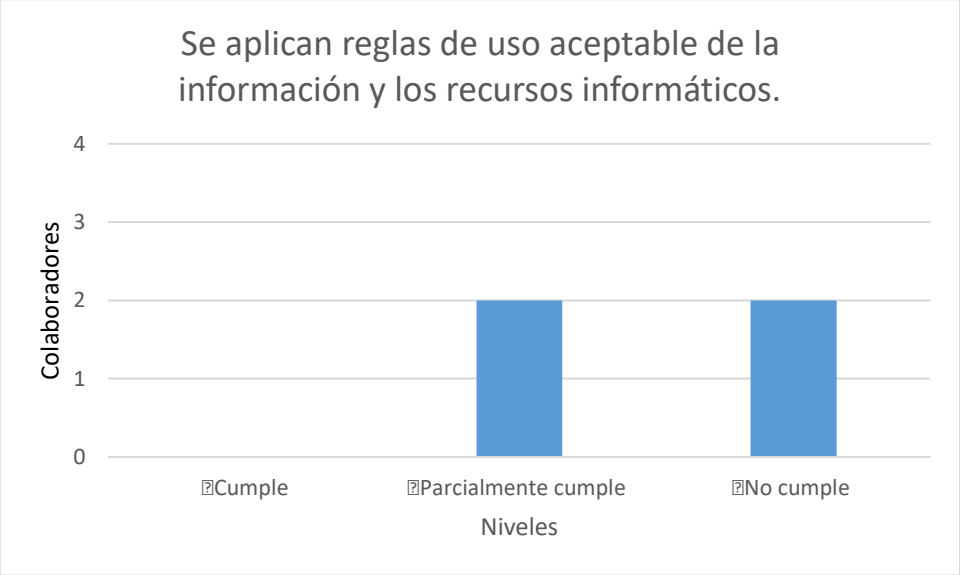
Ítem de evaluación N.º 04

Tabla 7
Uso y protección de la información

Niveles	Se aplican reglas de uso aceptable de la información y los recursos informáticos.
Cumple	0
Parcialmente cumple	2
No cumple	2
Total general	4

Fuente: Elaboración propia

Figura 4
Uso y protección de la información



Fuente: Elaboración propia

Nota: En el estudio contable JC TICONA se aplican prácticas básicas de uso responsable de la información, como el cuidado de contraseñas o la restricción de accesos externos; sin embargo, estas reglas son informales y no están documentadas.

Este hallazgo evidencia la necesidad de redactar y difundir un reglamento de uso aceptable de la información y de los recursos tecnológicos, conforme a la cláusula 5.10 de la ISO/IEC 27001:2022, que oriente el comportamiento del personal y promueva la seguridad digital.

Conclusión: Las normas existentes son empíricas y no cuentan con respaldo formal; se requiere establecer políticas escritas que regulen el uso de la información y los equipos.

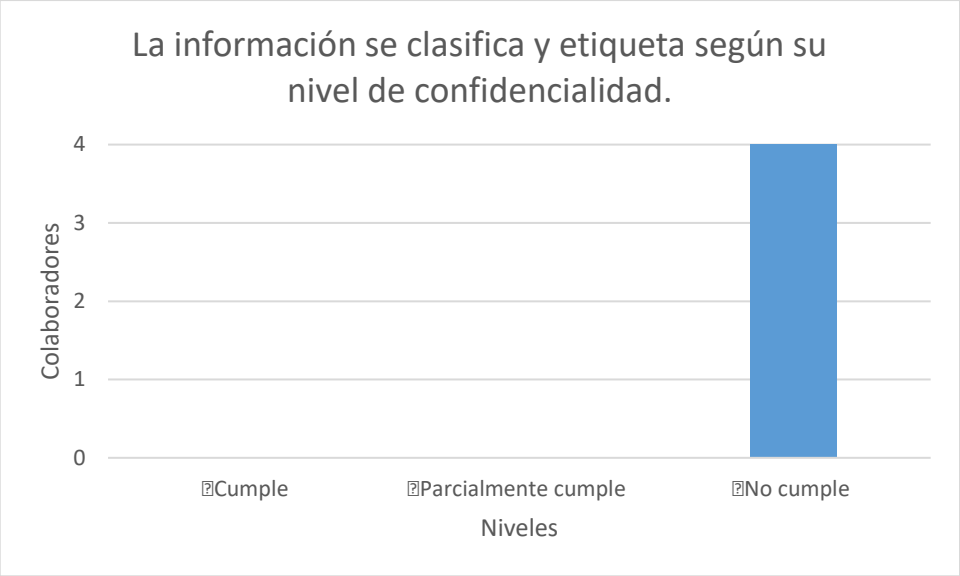
Ítem de evaluación N.º 05

Tabla *8*
Clasificación y etiquetado de la información

Niveles	La información se clasifica y etiqueta según su nivel de confidencialidad.
Cumple	0
Parcialmente cumple	0
No cumple	4
Total general	4

Nota. Elaboración propia

Figura 5
Clasificación y etiquetado de la información



Fuente: Elaboración propia

Nota: En el estudio contable JC TICONA no se clasifica la información según su nivel de confidencialidad. Los documentos se organizan por cliente o tipo de trámite, sin criterios de seguridad ni etiquetas que distingan la sensibilidad de los datos.

Este hallazgo evidencia la necesidad de implementar un sistema de clasificación y etiquetado de la información, conforme a las cláusulas 5.12 y 5.13 de la ISO/IEC 27001:2022, que establezca niveles de protección según el tipo de dato.

Conclusión: No existe un método de clasificación ni etiquetado; la información se gestiona de forma indiferenciada, exponiendo datos sensibles a posibles accesos indebidos.

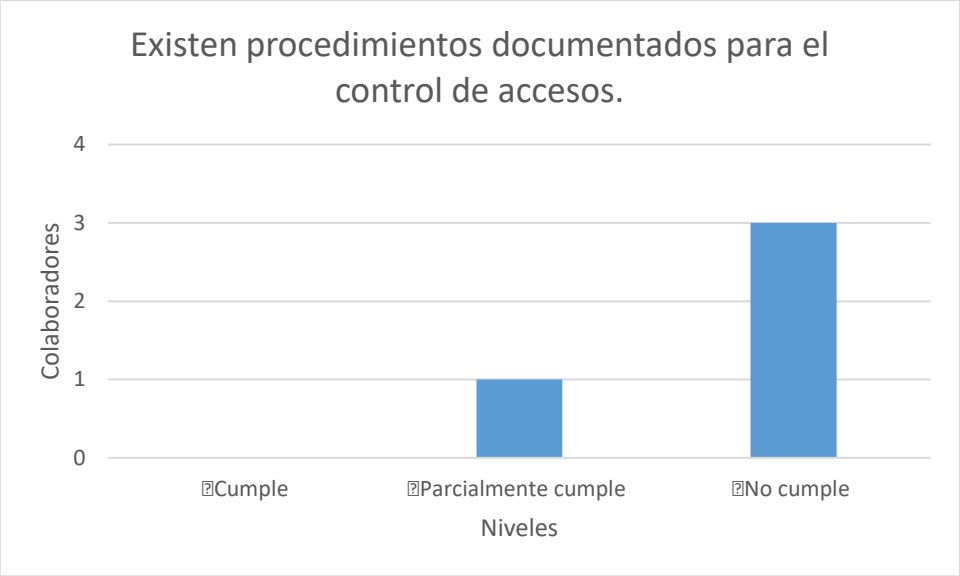
Ítem de evaluación N.º 06

Tabla 9
Procedimientos de acceso a la información

Niveles	Existen procedimientos documentados para el control de accesos.
Cumple	0
Parcialmente cumple	1
No cumple	3
Total general	4

Fuente: Elaboración propia

Figura 6
Procedimientos de acceso a la información



Fuente: Elaboración propia

Nota: En el estudio contable JC TICONA se utilizan contraseñas personales para el acceso a los sistemas contables y equipos informáticos; sin embargo, no existen procedimientos documentados para la creación, modificación o baja de usuarios.

Este hallazgo evidencia la necesidad de desarrollar procedimientos formales de control de accesos, conforme a las cláusulas 5.15 a 5.18 de la ISO/IEC 27001:2022, que regulen la administración de credenciales y revisiones periódicas de permisos.

Conclusión: Los controles de acceso se aplican de manera básica e informal; se requiere formalizar procedimientos que aseguren la protección y trazabilidad de las credenciales.

DOMINIO 2 – Riesgos y vulnerabilidades actuales (P2)

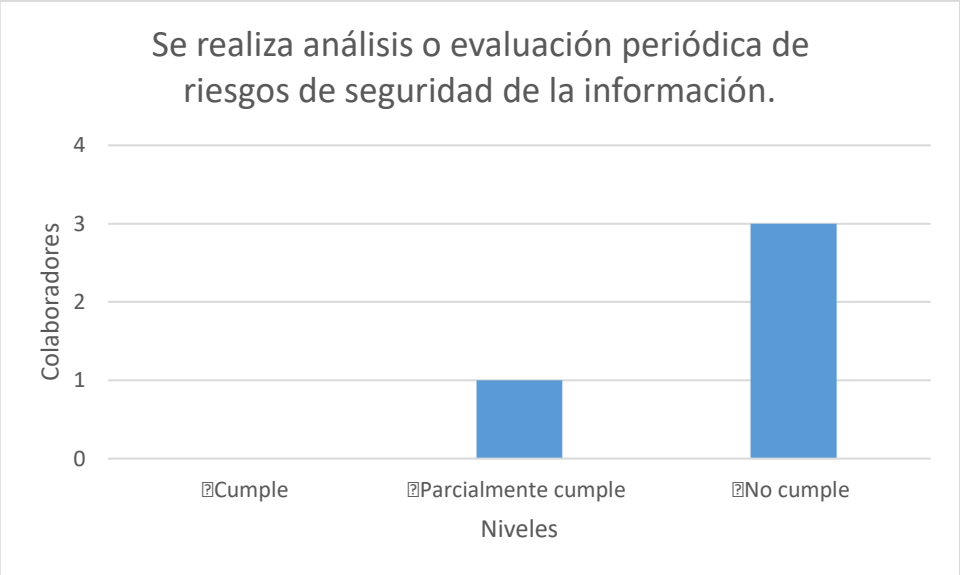
Ítem de evaluación N.º 07

Tabla 10
Identificación de vulnerabilidades

Niveles	Se realiza análisis o evaluación periódica de riesgos de seguridad de la información.
Cumple	0
Parcialmente cumple	1
No cumple	3
Total general	4

Fuente: Elaboración propia

Figura 7
Identificación de vulnerabilidades



Fuente: Elaboración propia

Nota: En el estudio contable JC TICONA no se realiza una evaluación formal ni periódica de los riesgos de seguridad de la información. Los incidentes se gestionan de manera reactiva, y las decisiones de protección se basan en la experiencia personal del contador jefe.

Este hallazgo evidencia la necesidad de implementar un proceso documentado de gestión de riesgos, conforme a la cláusula 6.1.2 de la ISO/IEC 27001:2022, que permita identificar, analizar y tratar las amenazas que puedan afectar la confidencialidad, integridad y disponibilidad de la información.

Conclusión: No existe un procedimiento estructurado de evaluación de riesgos; la organización actúa ante los problemas sin un enfoque preventivo ni sistemático.

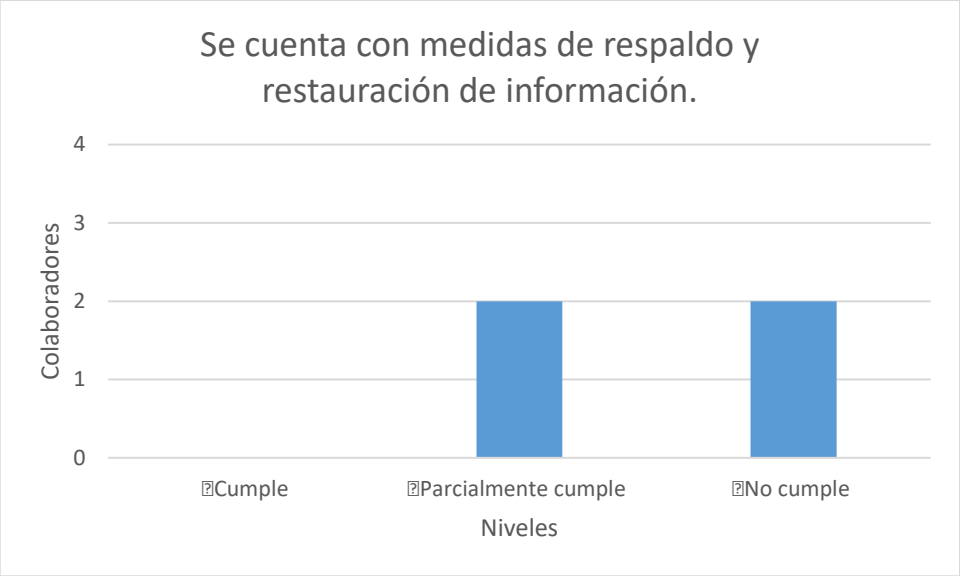
Ítem de evaluación N.º 08

Tabla 11
Controles de respaldo

Niveles	Se cuenta con medidas de respaldo y restauración de información.
Cumple	0
Parcialmente cumple	2
No cumple	2
Total general	4

Fuente: Elaboración propia

Figura 8
Controles de respaldo



Fuente: Elaboración propia

Nota: En el estudio contable JC TICONA se realizan copias manuales de respaldo en dispositivos externos, pero sin una periodicidad definida ni verificación de restauración. No existen políticas o procedimientos que regulen estas actividades.

Este hallazgo evidencia la necesidad de establecer un sistema de respaldo y recuperación formal, conforme a la cláusula **8.13** de la **ISO/IEC 27001:2022**, que garantice la disponibilidad de la información ante fallas técnicas o pérdidas accidentales.

Conclusión: El respaldo de información se realiza de forma empírica y sin control; es necesario documentar y automatizar el proceso para asegurar la continuidad operativa.

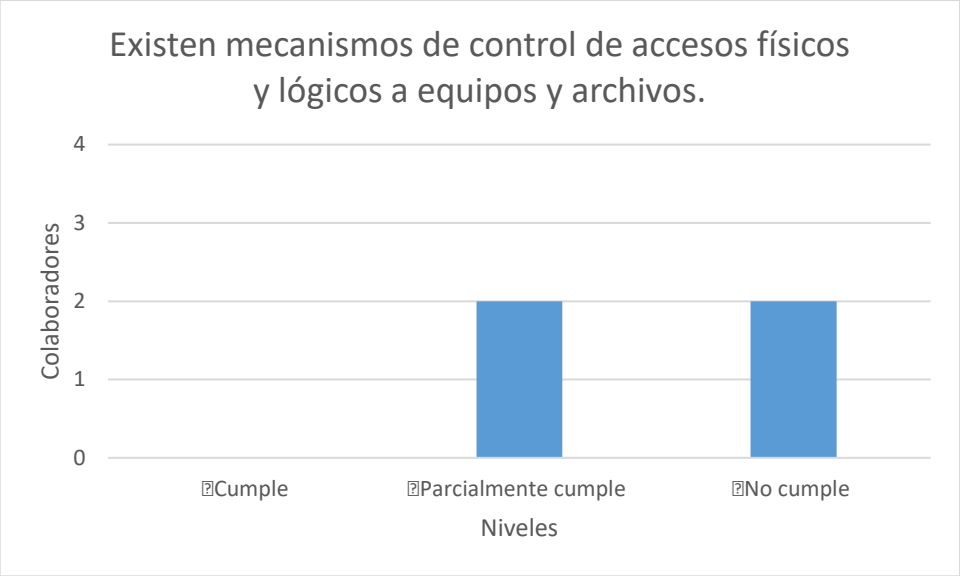
Ítem de evaluación N.º 09

Tabla 12
Control de accesos

Niveles	Existen mecanismos de control de accesos físicos y lógicos a equipos y archivos.
Cumple	0
Parcialmente cumple	2
No cumple	2
Total general	4

Fuente: Elaboración propia

Figura 9
Control de accesos



Fuente: Elaboración propia

Nota: En el estudio contable JC TICONA se restringe el acceso físico a los equipos solo durante el horario laboral, pero no existen cerraduras ni sistemas de registro de ingreso. El control lógico se limita al uso de contraseñas individuales sin supervisión ni revisión periódica.

Este hallazgo evidencia la necesidad de implementar controles de acceso físico y lógico, conforme a las cláusulas 7.2 y 8.3 de la ISO/IEC 27001:2022, que definan mecanismos de protección, autenticación y trazabilidad en el manejo de información sensible.

Conclusión: Los controles existentes son básicos e informales; se requiere definir procedimientos formales de acceso físico y lógico que garanticen la seguridad integral de los activos.

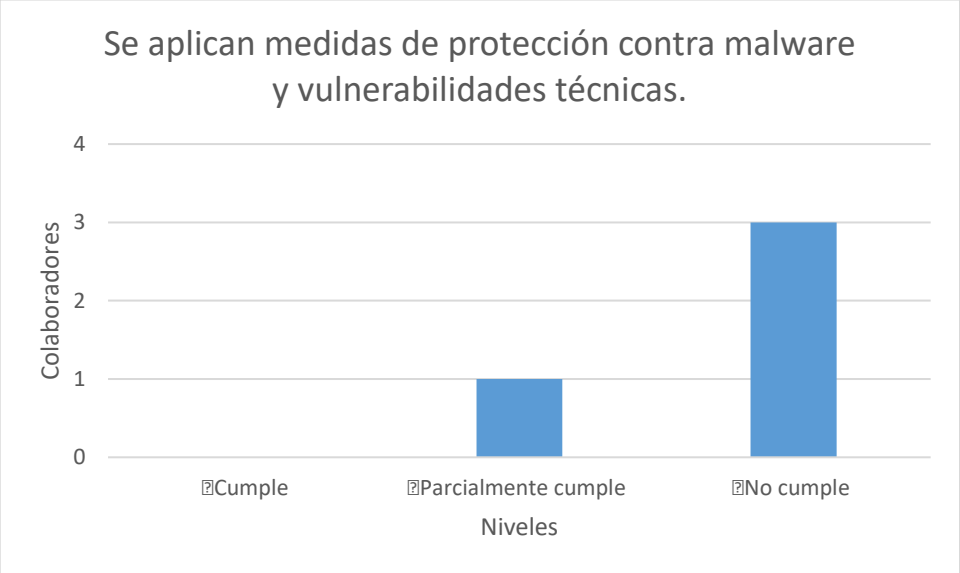
Ítem de evaluación N.º 10

Tabla 13
Protección contra vulnerabilidades

Niveles	Se aplican medidas de protección contra malware y vulnerabilidades técnicas.
Cumple	0
Parcialmente cumple	1
No cumple	3
Total general	4

Fuente: Elaboración propia

Figura 10
Protección contra vulnerabilidades



Fuente: Elaboración propia

Nota: En el estudio contable JC TICONA se utilizan programas antivirus en los equipos principales, aunque no se realizan análisis automáticos ni actualizaciones regulares. Algunos dispositivos carecen de protección activa.

Este hallazgo evidencia la necesidad de establecer políticas de protección contra software malicioso y gestión de vulnerabilidades, conforme a las cláusulas 8.7 y 8.8 de la ISO/IEC 27001:2022, para fortalecer la defensa tecnológica y minimizar riesgos de intrusión.

Conclusión: La protección contra malware se aplica parcialmente; se requiere un control centralizado de actualizaciones y monitoreo de vulnerabilidades.

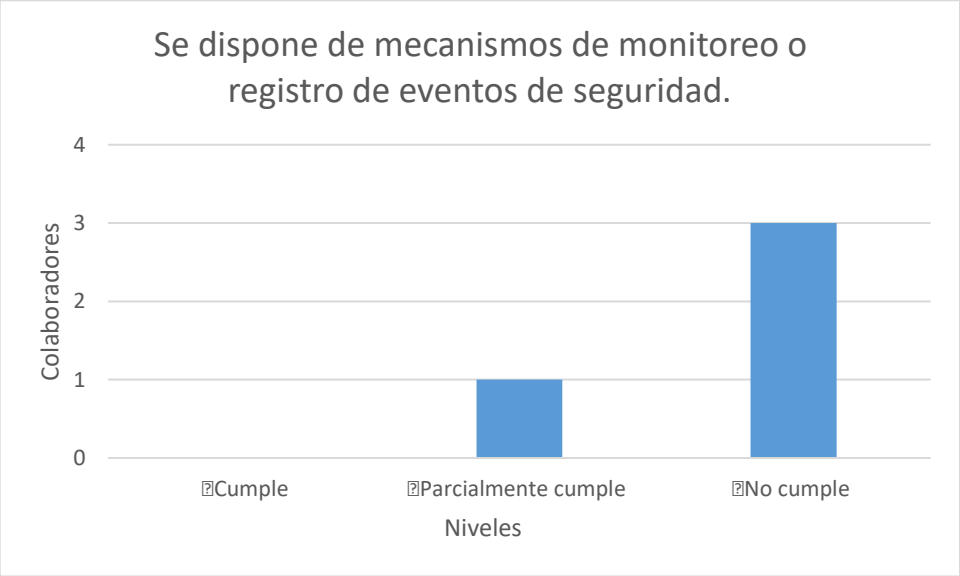
Ítem de evaluación N.º 11

Tabla 14
Registro de incidentes

Niveles	Se dispone de mecanismos de monitoreo o registro de eventos de seguridad.
Cumple	0
Parcialmente cumple	1
No cumple	3
Total general	4

Fuente: Elaboración propia

Figura 11
Registro de incidentes



Fuente: Elaboración propia

Nota: En el estudio contable JC TICONA no existen registros sistemáticos de eventos o incidentes de seguridad. Los problemas se resuelven verbalmente sin documentación ni trazabilidad.

Este hallazgo evidencia la necesidad de establecer mecanismos de registro y monitoreo de incidentes, conforme a las cláusulas 8.15 y 8.16 de la ISO/IEC 27001:2022, que permitan la detección temprana y análisis de incidentes.

Conclusión: No se dispone de un sistema de monitoreo ni de registros de eventos; la respuesta a incidentes se gestiona de manera reactiva e informal.

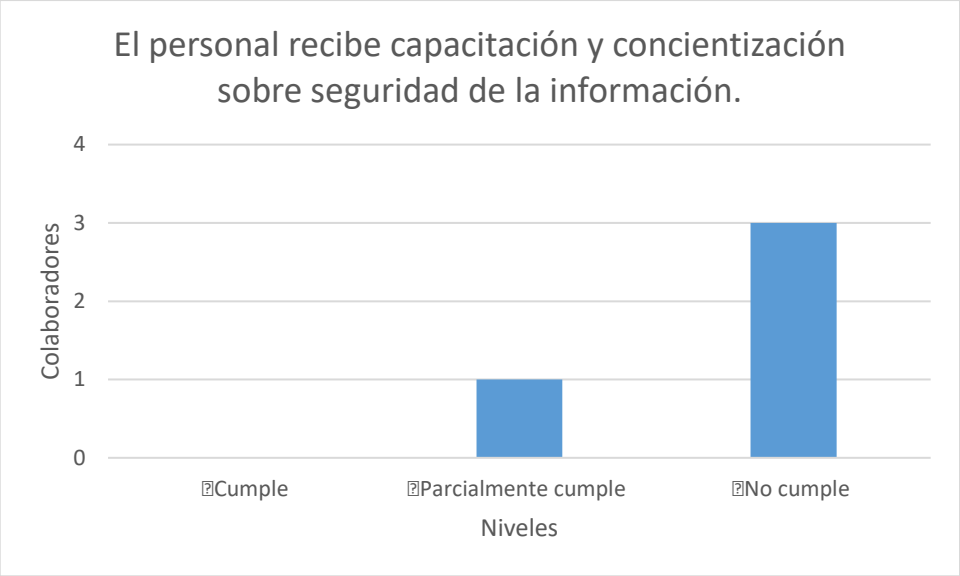
Ítem de evaluación N.º 12

Tabla 15
Capacitación en riesgos

Niveles	El personal recibe capacitación y concientización sobre seguridad de la información.
Cumple	0
Parcialmente cumple	1
No cumple	3
Total general	4

Fuente: Elaboración propia

Figura 12
Capacitación en riesgos



Fuente: Elaboración propia

Nota: En el estudio contable JC TICONA no se desarrollan capacitaciones formales sobre seguridad de la información. Solo se dan orientaciones verbales ocasionales al incorporar nuevo personal.

Este hallazgo evidencia la necesidad de implementar un programa de concientización continua, conforme a la cláusula 6.3 de la ISO/IEC 27001:2022, que fortalezca la cultura de seguridad y la responsabilidad del personal en la protección de los datos.

Conclusión: La concientización del personal es insuficiente; se requiere un plan de capacitación estructurado y permanente en seguridad de la información.

DOMINIO 3 – Lineamientos para el diseño de políticas (P3)

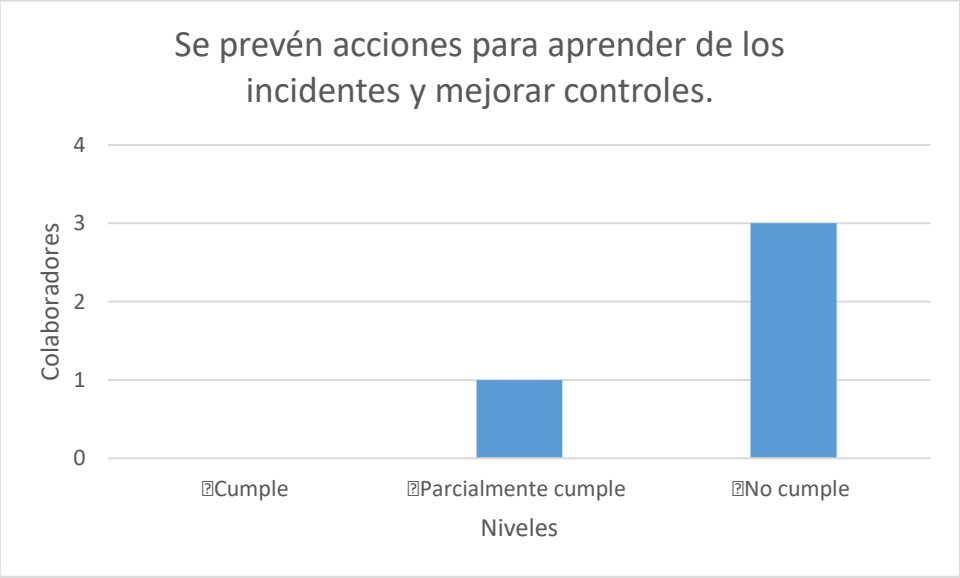
Ítem de evaluación N.º 13

Tabla 16
Procedimientos mínimos establecidos

Niveles	Se prevén acciones para aprender de los incidentes y mejorar controles.
Cumple	0
Parcialmente cumple	1
No cumple	3
Total general	4

Fuente: Elaboración propia

Figura 13
Procedimientos mínimos establecidos



Fuente: Elaboración propia

Nota: En el estudio contable JC TICONA no existe un procedimiento formal para la gestión de incidentes de seguridad. Los problemas se comunican verbalmente y se solucionan de manera empírica, sin registro ni trazabilidad.

Este hallazgo evidencia la necesidad de desarrollar un plan de gestión de incidentes que contemple detección, análisis, respuesta y registro de eventos, conforme a las cláusulas

5.24 a 5.26 de la ISO/IEC 27001:2022, garantizando la respuesta oportuna y la mejora continua del sistema.

Conclusión: No existe una planificación estructurada para la gestión de incidentes; las acciones se ejecutan sin control ni documentación formal.

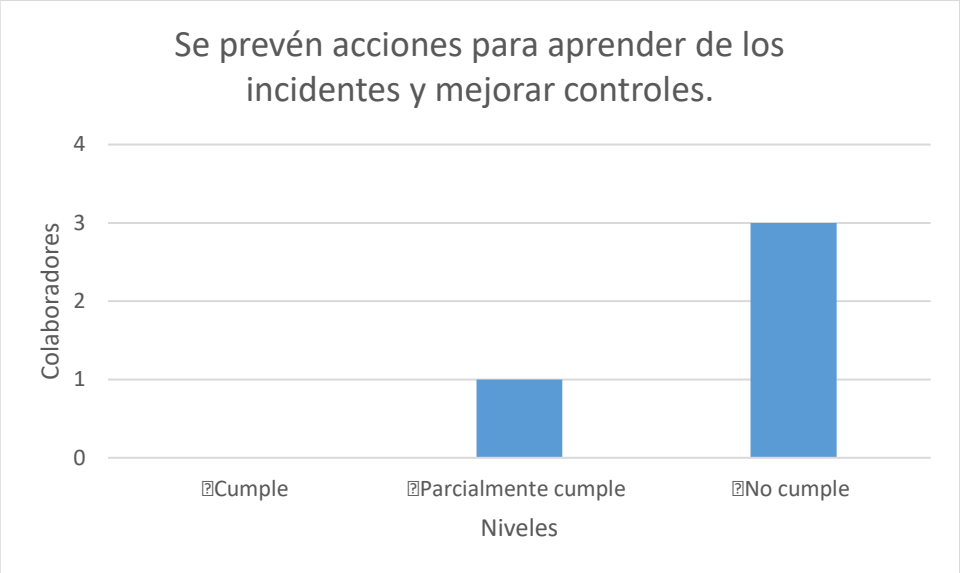
Ítem de evaluación N.º 14

Tabla 17
Controles esenciales implementados

Niveles	Se prevén acciones para aprender de los incidentes y mejorar controles.
Cumple	0
Parcialmente cumple	1
No cumple	3
Total general	4

Fuente: Elaboración propia

Figura 14
Controles esenciales implementados



Fuente: Elaboración propia

Nota: En el estudio contable JC TICONA no se realizan revisiones posteriores a los incidentes ni se documentan las causas o lecciones aprendidas. Las soluciones se limitan a corregir el problema inmediato sin análisis posterior.

Este hallazgo evidencia la necesidad de implementar un proceso de revisión postincidente, conforme a la cláusula 5.27 de la ISO/IEC 27001:2022, para identificar oportunidades de mejora y evitar recurrencias.

Conclusión: No se aplican acciones de aprendizaje ni mejora tras los incidentes; la organización carece de retroalimentación formal para fortalecer sus controles.

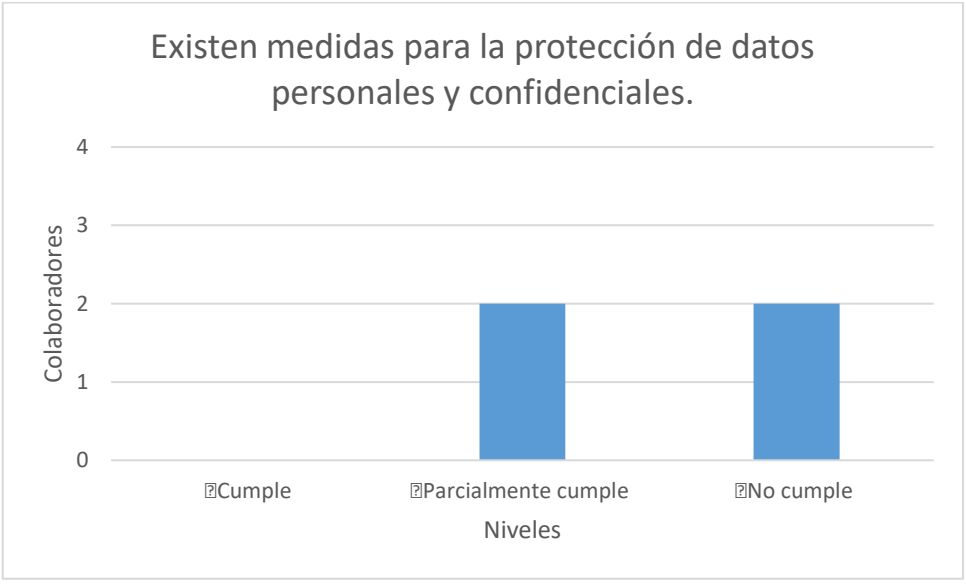
Ítem de evaluación N.º 15

Tabla 18
Gestión de activos de información

Niveles	Existen medidas para la protección de datos personales y confidenciales.
Cumple	0
Parcialmente cumple	2
No cumple	2
Total general	4

Fuente: Elaboración propia

Figura 15
Gestión de activos de información



Fuente: Elaboración propia

Nota: En el estudio contable JC TICONA se resguardan los documentos físicos en archivadores bajo llave, pero los archivos digitales carecen de cifrado y se almacenan en dispositivos personales. No existen políticas específicas sobre la protección de datos personales o confidenciales.

Este hallazgo evidencia la necesidad de establecer procedimientos y controles técnicos para la protección de datos, conforme a la cláusula 5.34 de la ISO/IEC 27001:2022, garantizando el cumplimiento de los principios de confidencialidad y privacidad. **Conclusión:** Las medidas de protección son parciales y se concentran en el ámbito físico; se requiere formalizar políticas de seguridad digital para la protección de datos personales.

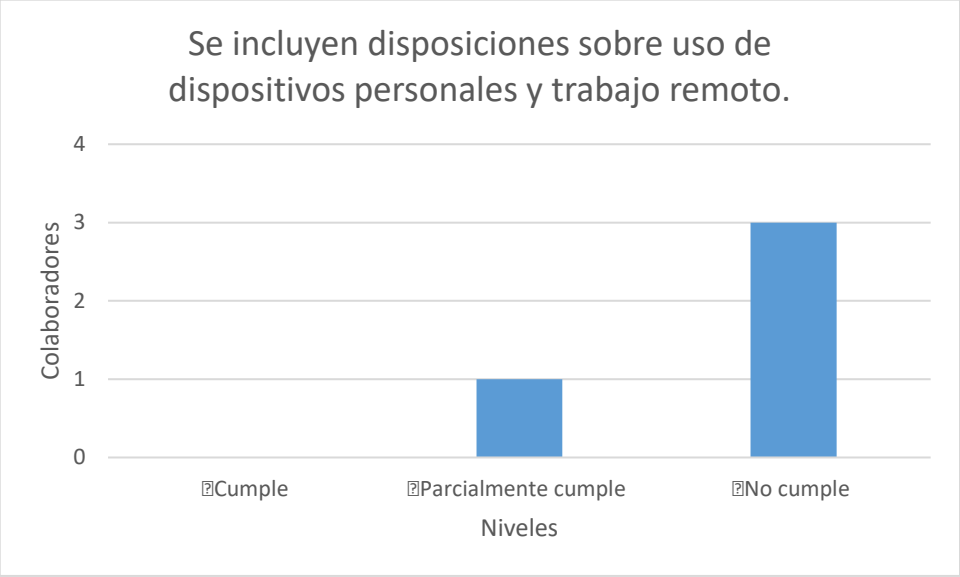
Ítem de evaluación N.º 16

Tabla 19
Responsable de seguridad

Niveles	Se incluyen disposiciones sobre uso de dispositivos personales y trabajo remoto.
Cumple	0
Parcialmente cumple	1
No cumple	3
Total general	4

Fuente: Elaboración propia

Figura 16
Responsable de seguridad



Fuente: Elaboración propia

Nota: En el estudio contable JC TICONA algunos colaboradores utilizan dispositivos personales para acceder a información contable desde sus hogares, sin lineamientos formales ni medidas de control remoto.

Este hallazgo evidencia la necesidad de incorporar políticas específicas sobre el uso de equipos personales y trabajo remoto, conforme a las cláusulas 6.7 y 8.1 de la ISO/IEC 27001:2022, que regulen el acceso seguro a los sistemas de información desde entornos externos.

Conclusión: No existen directrices formales para el uso de dispositivos personales ni trabajo remoto; se requiere definir políticas que minimicen riesgos de exposición de datos.

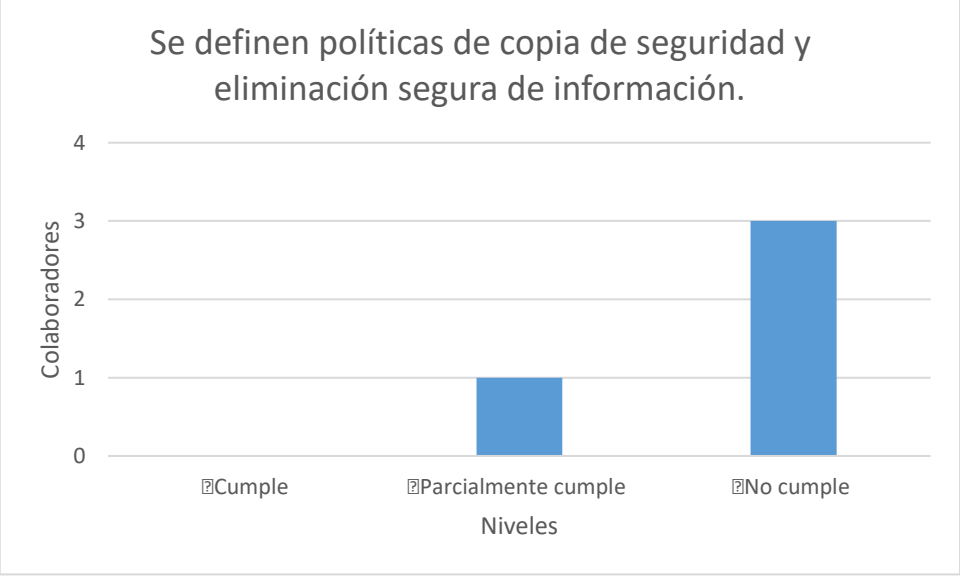
Ítem de evaluación N.º 17

Tabla 20
Prácticas de mejora continua

Niveles	Se definen políticas de copia de seguridad y eliminación segura de información.
Cumple	0
Parcialmente cumple	1
No cumple	3
Total general	4

Fuente: Elaboración propia

Figura 17
Prácticas de mejora continua



Fuente: Elaboración propia

Nota: En el estudio contable JC TICONA se realizan copias de respaldo ocasionales, pero no existe una política documentada ni procedimientos de eliminación segura de información obsoleta.

Este hallazgo evidencia la necesidad de establecer políticas claras de respaldo y eliminación segura, conforme a las cláusulas 8.13 y 7.14 de la ISO/IEC 27001:2022, que aseguren la disponibilidad y confidencialidad de los datos a lo largo de su ciclo de vida.

Conclusión: No hay políticas formales sobre respaldo ni eliminación; las prácticas son improvisadas y carecen de control técnico.

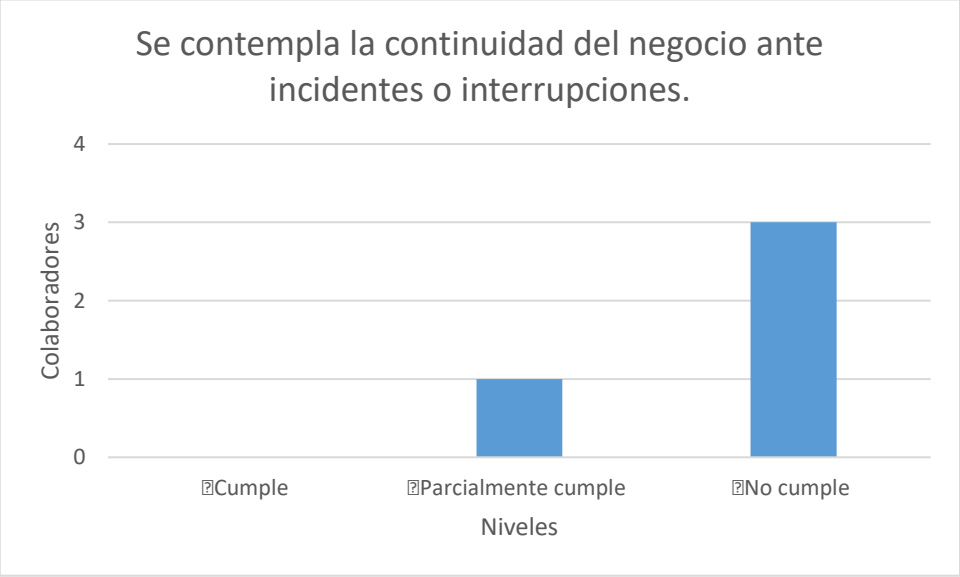
Ítem de evaluación N.º 18

Tabla 21
Continuidad operativa

Niveles	Se contempla la continuidad del negocio ante incidentes o interrupciones.
Cumple	0
Parcialmente cumple	1
No cumple	3
Total general	4

Fuente: Elaboración propia

Figura 18
Continuidad operativa



Fuente: Elaboración propia

Nota: En el estudio contable JC TICONA no existe un plan documentado de continuidad del negocio. Las contingencias se afrontan reprogramando tareas o usando equipos alternos, sin estrategias de recuperación definidas

Este hallazgo evidencia la necesidad de diseñar un plan de continuidad que contemple escenarios de emergencia, conforme a la cláusula 5.30 de la ISO/IEC 27001:2022, para mantener la operación ante fallos o incidentes críticos.

Conclusión: No se cuenta con un plan de continuidad; las acciones de recuperación son improvisadas y carecen de planificación preventiva.

4.4.5. Resumen general del nivel de cumplimiento de los controles de seguridad de la información

El análisis global de los 18 ítems evaluados en los tres dominios de la lista de cotejo evidencia que el estudio contable JC TICONA presenta un nivel de cumplimiento formal nulo respecto a los requisitos de la norma ISO/IEC 27001:2022, dado que ningún control obtuvo la categoría “Cumple” (0 %). Asimismo, se observa que el 88.9 % de los controles se clasifican como “Parcialmente cumple”, lo que refleja que la mayoría de procedimientos se realizan de manera empírica, sin documentación, estandarización ni responsables definidos. Finalmente, el 11.1 % de los controles se categorizan como “No cumple”, destacándose brechas críticas en la clasificación de la información y en la gestión del inventario de activos. Estos resultados confirman la necesidad urgente de implementar políticas, procedimientos y lineamientos formales que garanticen la seguridad de la información y la continuidad operativa del estudio.

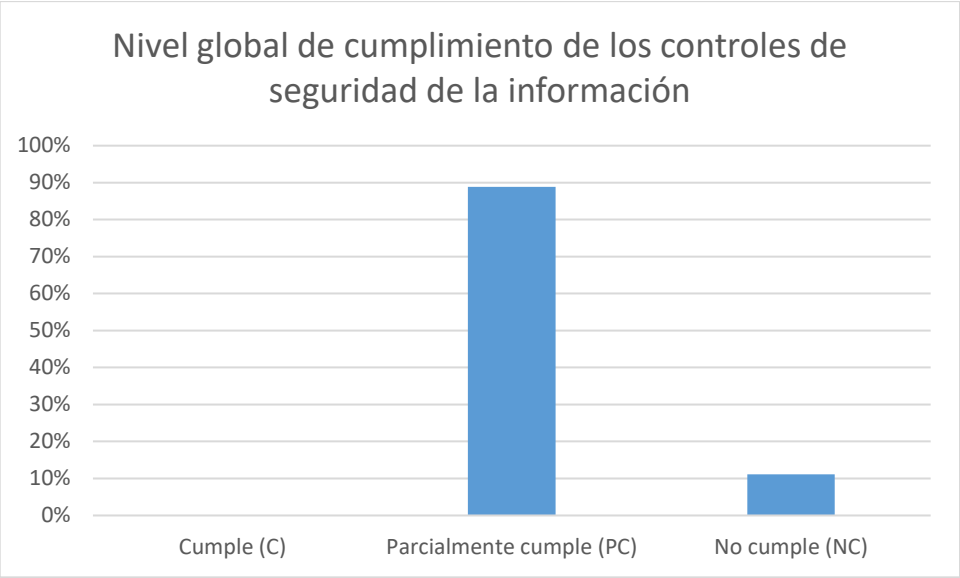
Tabla 22
Análisis global de los 18 ítems evaluados

Nivel global de cumplimiento de los controles de seguridad de la información

Categoría de evaluación	Ítems con esa condición	Porcentaje (%)
Cumple (C)	0	0%
Parcialmente cumple (PC)	16	88.90%
No cumple (NC)	2	11.10%
Total	18	100%

Fuente: Elaboración propia

Figura 19
Nivel global de cumplimiento de los controles de seguridad de la información



Fuente: Elaboración propia

5. PROPUESTA DE INNOVACIÓN

5.1. Alcance esperado

La propuesta tiene como finalidad establecer un marco de referencia para el diseño de políticas de seguridad de la información en el estudio contable JC TICONA, tomando como base los lineamientos de la ISO/IEC 27001:2022 y los resultados del diagnóstico realizado sobre el nivel de cumplimiento de la norma. El alcance del proyecto se centra en traducir los hallazgos de la evaluación en un conjunto de lineamientos y componentes mínimos que deberán considerar las futuras políticas formales del estudio.

En esa línea, el trabajo no implementa un sistema de gestión de seguridad de la información ni desarrolla un manual definitivo, sino que define la estructura general, los ejes temáticos y las prioridades que servirán como insumo para la posterior elaboración, documentación y validación interna de dichas políticas por parte de la organización.

Los resultados esperados serán:

- La identificación detallada de brechas y riesgos críticos derivados de la ausencia de políticas formales de seguridad de la información, obtenida mediante la aplicación de la lista de cotejo basada en la ISO/IEC 27001:2022.
- La formulación de un conjunto de lineamientos conceptuales que definan los componentes mínimos que deberán incorporar las futuras políticas de seguridad de la información, incluyendo aspectos como control de accesos, uso aceptable, respaldo y recuperación de datos, gestión de incidentes y continuidad operativa.
- El planteamiento de una ruta referencial para que el estudio contable JC TICONA pueda elaborar e implementar, en una etapa posterior, su manual formal de políticas de seguridad de la información, considerando prioridades, fases y criterios generales.

5.2. Descripción del mercado objetivo del producto o servicio

El mercado objetivo del producto se orienta, en primer lugar, al cliente interno primario, representado por el estudio contable JC TICONA, ubicado en la ciudad de Tacna. Asimismo, se considera un cliente externo potencial y escalable a las micro y pequeñas empresas contables, así como por estudios de servicios profesionales del sur del Perú que requieren políticas mínimas de seguridad de la información.

5.2.1. Fuentes de ingreso

La empresa asumirá directamente los costos de diseño de políticas, capacitación del personal, adquisición de software de respaldo y antivirus, así como la impresión y difusión del manual, integrándolos en su presupuesto operativo. En esta fase, no se proyectará un flujo de ingresos adicional, dado que la propuesta tendrá como finalidad principal fortalecer la seguridad de la información y la continuidad operativa del estudio.

5.2.2. Canales de distribución

Los canales de distribución del servicio se estructurarán en tres modalidades complementarias. En primer lugar, se utilizará un canal directo, mediante la prestación de servicios de consultoría y acompañamiento presencial o remoto al estudio contable JC TICONA. En segundo lugar, se implementará un canal digital, a través de redes sociales profesionales, correo institucional y la página web del estudio, con el propósito de ofrecer el servicio a terceros interesados. Finalmente, se considerará un canal académico, basado en alianzas con instituciones técnicas o universitarias, que permitirán replicar el modelo como práctica profesional de innovación en seguridad de la información.

5.2.3. Estrategias de penetración en el mercado

Las estrategias de penetración en el mercado se orientarán a posicionar la propuesta como una solución técnica confiable y replicable en el sector de servicios contables. En primer lugar, se desarrollará la demostración de resultados, mediante la documentación del estudio contable JC TICONA como caso de referencia, lo que permitirá evidenciar mejoras en la gestión de la seguridad de la información. En segundo lugar, se implementará una oferta escalonada de servicios, que contemplará diagnósticos de seguridad de bajo costo para micro y pequeñas empresas, con el fin de facilitar el acceso inicial a la solución. Finalmente, se desarrollarán acciones de promoción académica y educativa, tales como charlas, seminarios virtuales y materiales informativos sobre los riesgos de no contar con políticas de seguridad de la información, con el propósito de sensibilizar a potenciales usuarios y tomadores de decisión.

5.2.4. Alianzas estratégicas

Las alianzas estratégicas se constituirán como un componente clave para la sostenibilidad y escalabilidad de la propuesta. Se promoverán convenios de colaboración con los Colegios de Contadores Públicos de Tacna y Arequipa, a fin de difundir la importancia de las políticas de seguridad de la información en los estudios contables y respaldar la adopción del modelo propuesto. Asimismo, se gestionarán alianzas con empresas tecnológicas y proveedores de software contable, con el propósito de incorporar controles de acceso, respaldo y otras funcionalidades alineadas con las políticas de seguridad diseñadas. Finalmente, se coordinará con entidades del Estado, como PRODUCE o INDECOPI, para articular la propuesta con programas de formalización digital y cumplimiento normativo, lo que reforzará su legitimidad y su potencial de réplica en otras organizaciones.

5.2.5. Benchmarking

5.3. Desarrollo del proyecto de innovación

Etapa 1: Diagnostico del nivel de cumplimiento y análisis de brechas

En esta etapa, la propuesta plantea que el estudio contable realizará un diagnóstico técnico y organizacional integral, articulado sobre la norma ISO/IEC 27001:2022, con el objetivo de conocer el estado real de la seguridad de la información y su nivel de cumplimiento. El diagnóstico será ejecutado por un profesional con formación en redes y seguridad de la información, incorporando criterios técnicos que permitan identificar riesgos vinculados al tratamiento de información tributaria, financiera y de datos personales de clientes.

Como producto de esta etapa, el estudio contará con:

- Matriz de evaluación de cumplimiento con escala “Cumple”, “Parcialmente cumple” o “No cumple”.
- Inventario de activos físicos, digitales y de información.
- Mapa lógico de red y de flujo de información.
- Reporte de brechas priorizadas según criticidad e impacto.

- **Diagnóstico documental y normativo**

El estudio contable evaluará la existencia, vigencia y calidad de los documentos que regulan su operación y su relación con la seguridad de la información. En particular:

- Se revisará la documentación asociada a procesos contables y administrativos críticos, tales como la recepción y archivo de comprobantes de pago electrónicos, la elaboración de planillas y beneficios sociales, la conciliación bancaria, la elaboración de reportes financieros, y la gestión documental por cliente.
- Se verificará la presencia o ausencia de políticas internas relacionadas con seguridad de la información, confidencialidad, protección de datos personales, control de accesos y uso de recursos tecnológicos.
- Se analizará cómo se desarrollan las prácticas reales de trabajo, contrastando lo documentado con lo ejecutado, para identificar procesos informales, dependientes de la experiencia individual o de costumbres no estandarizadas.

Este diagnóstico permitirá detectar brechas normativas y documentales, especialmente en controles que requieren formalización, evidencias de cumplimiento y asignación de responsabilidades.

- **Diagnóstico técnico de infraestructura**

El diagnóstico técnico contemplará un levantamiento completo de la infraestructura de redes, equipos, sistemas, almacenamiento y mecanismos de protección, enfocándose en los activos que soportan el trabajo contable.

- **Mapa lógico de red**

El estudio realizará un levantamiento de la red interna con el fin de conocer su estructura, puntos de acceso, rutas de comunicación y exposición. Este levantamiento incluirá:

- Identificación del equipo de enrutamiento principal, verificando capacidades de seguridad, configuración de red, restricciones de acceso administrativo y servicios activos.
- Identificación de equipos de conmutación (switches), verificando si permiten segmentación, el estado del cableado y la exposición física de puntos de red.
- Identificación de los puntos de acceso de red inalámbrica, verificando el tipo de cifrado, el alcance de señal, la existencia de redes separadas para personal y visitantes, y el control de acceso inalámbrico.
- Elaboración de un diagrama lógico donde se representen los equipos críticos, estaciones de trabajo, impresoras conectadas a red, y puntos de almacenamiento o compartición de archivos.

Asimismo, se realizará un análisis de segmentación, verificando si la red interna donde se gestiona información contable se encuentra separada de una red destinada a visitantes o dispositivos ajenos a la operación. Esta revisión buscará reducir el riesgo de accesos no autorizados y propagación de software malicioso dentro de la red interna.

Finalmente, se revisarán configuraciones críticas, tales como el cifrado de la red inalámbrica (por ejemplo, estándares modernos de cifrado), las credenciales de

administración de equipos de red y la presencia de servicios habilitados que no sean estrictamente necesarios para la operación.

- **Inventario físico y digital**

El estudio elaborará un inventario que incluirá:

- Equipos de cómputo, computadoras portátiles, impresoras conectadas a red y dispositivos móviles utilizados para fines operativos del estudio.
- Programas informáticos de contabilidad, programas de facturación electrónica, herramientas ofimáticas, soluciones antivirus, y aplicaciones de almacenamiento en la nube.
- Medios de almacenamiento utilizados, tales como servicios de almacenamiento en la nube, discos duros externos, carpetas compartidas en red interna y otros repositorios de información.

Este inventario permitirá identificar activos críticos, responsables de uso y el tipo de información que cada activo almacena o procesa.

- **Controles técnicos básicos**

El estudio verificará la existencia y estado de controles técnicos mínimos, entre ellos:

- Estado de protección antivirus y antimalware en cada equipo, incluyendo vigencia y actualización.
- Uso de cuentas de usuario individuales frente a cuentas compartidas, para asegurar trazabilidad y responsabilidad.
- Existencia de permisos diferenciados para carpetas y archivos contables, evitando accesos indiscriminados a información de clientes.
- Forma actual de intercambio de información entre colaboradores, evaluando el uso de memorias externas, mensajería instantánea, correo electrónico y servicios de almacenamiento en la nube.

Esta revisión permitirá determinar el nivel de exposición frente a pérdida de información, fuga de datos o alteración no autorizada.

- **Validación real de respaldos**

La propuesta establece que el estudio deberá verificar la existencia real de copias de seguridad y su capacidad de recuperación, no solo su existencia declarada. Para ello:

- Se comprobará si se realizan copias de seguridad de información crítica, como libros contables electrónicos, declaraciones tributarias, registros de planillas, archivos de facturación electrónica y documentación de clientes.
- Se verificará la ubicación del respaldo (por ejemplo, disco externo o almacenamiento en la nube) y su nivel de protección.
- Se ejecutará una restauración controlada de archivos seleccionados para comprobar integridad, accesibilidad y utilidad real.
- Se evaluará si los respaldos están protegidos contra eventos comunes, como fallas de equipos o ataques de software malicioso que cifre archivos.
- **Construcción del mapa de brechas**

Con base en los hallazgos documentales y técnicos, el estudio consolidará un mapa de brechas que identifique:

- Brechas críticas: controles inexistentes o con ausencia total de formalización.
- Brechas técnicas: configuraciones inseguras, falta de segmentación, debilidad en controles de acceso o exposición de información por prácticas tecnológicas inadecuadas.
- Brechas operativas: procesos manuales sin control, uso no regulado de memorias externas o canales informales de intercambio de información.
- Brechas normativas: ausencia de políticas internas, falta de clasificación de información, inexistencia de gestión de incidentes o continuidad operativa mínima.

Este mapa será el punto de partida para formular lineamientos conceptuales y una ruta de formalización.

Etapa 2: Formulación de lineamientos conceptuales para el diseño de políticas

En esta etapa, la propuesta plantea que el estudio contable transformará las brechas identificadas en lineamientos conceptuales técnicos y organizacionales que servirán como

base para la futura elaboración de políticas internas de seguridad de la información. Estos lineamientos no constituyen todavía un manual formal, sino un conjunto de criterios mínimos que deben incorporarse para controlar riesgos reales.

Como producto de esta etapa, el estudio contará con un documento de lineamientos organizados por dominios: control de accesos, protección de datos, respaldo y recuperación, gestión de incidentes y continuidad operativa.

Lineamientos para el control de accesos

El estudio definirá criterios para regular el acceso a información y sistemas, considerando roles y funciones. Los lineamientos deberán establecer:

- Perfiles diferenciados para gerencia, contadores, asistentes, practicantes y soporte técnico, según responsabilidades reales.
- Reglas obligatorias para el uso de credenciales seguras, prohibiendo compartir contraseñas o usar cuentas genéricas sin trazabilidad.
- Control de acceso a carpetas y archivos críticos, especialmente aquellos que contienen información de clientes, libros contables, planillas, reportes financieros y declaraciones tributarias.
- Procedimientos para creación, modificación y eliminación de accesos cuando ingresa o se retira personal del estudio.

Lineamientos de manejo y protección de datos

El estudio establecerá reglas mínimas de protección de información, considerando la sensibilidad de los datos. Estos lineamientos incluirán:

- Regulación del uso de memorias externas y dispositivos de almacenamiento portátiles, ya sea restringiendo su uso o sometiéndolo a control y verificación previa.
- Reglas para el envío y compartición de archivos mediante correo electrónico, almacenamiento en la nube y mensajería instantánea, evitando exposiciones por enlaces públicos o reenvíos sin control.
- Prohibición de almacenar información contable y de clientes en equipos personales no autorizados, salvo bajo condiciones controladas.
- Clasificación de información en niveles (por ejemplo: pública, interna y confidencial) y reglas operativas asociadas a cada nivel.

Lineamientos de respaldo y recuperación

El estudio definirá criterios mínimos para asegurar disponibilidad e integridad de la información:

- Frecuencia mínima de copias de seguridad según criticidad: procesos tributarios y contables deberán contar con respaldos más frecuentes que documentos de soporte.
- Uso combinado de almacenamiento en la nube y almacenamiento externo, reduciendo el riesgo de pérdida por fallas locales.
- Pruebas periódicas de restauración para verificar que los respaldos son recuperables.
- Identificación explícita de información que no puede perderse, como libros contables electrónicos, declaraciones presentadas, archivos de facturación electrónica y documentación esencial de clientes.

Lineamientos de gestión de incidentes

El estudio establecerá criterios para gestionar eventos de seguridad que afecten información, equipos o continuidad del servicio. Se definirán:

- Qué situaciones se consideran incidentes (por ejemplo: infección de software malicioso, pérdida de archivos, acceso no autorizado, envío erróneo de información de un cliente a otro, robo o pérdida de equipos).
- Pasos mínimos de actuación: contención, registro del incidente, análisis de causa, acción correctiva y lecciones aprendidas.
- Responsabilidades por rol: quién reporta, quién decide acciones, y quién ejecuta medidas técnicas.

Lineamientos de continuidad operativa

El estudio deberá prever escenarios de interrupción que afecten el cumplimiento tributario y la atención a clientes. Por ello:

- Se definirán acciones ante fallas de equipos críticos, caídas de red interna o interrupciones de Internet.
- Se establecerán alternativas temporales para continuar trabajando, incluyendo equipos de reemplazo, acceso remoto controlado o procedimientos de trabajo sin conexión cuando sea viable.
- Se identificarán procesos críticos por fecha y prioridad, de modo que ante una interrupción se atienda primero lo indispensable para cumplimiento y continuidad.

Estos lineamientos conformarán el marco técnico-organizacional previo al manual formal.

Etapa 3: Planteamiento de una ruta referencial para la futura elaboración del manual

En esta etapa, la propuesta definirá un camino secuencial para que el estudio contable pueda elaborar, validar y poner en funcionamiento un manual formal de políticas de seguridad de la información, tomando como base los lineamientos previos. La finalidad es evitar que las políticas queden como documentos teóricos, y asegurar que sean aplicables al tamaño, recursos y operatividad real del estudio.

Fase de organización

El estudio formalizará la necesidad del manual mediante comunicación interna y asignación de responsabilidades. Se designará un responsable técnico de redes y seguridad y un responsable operativo contable para co-desarrollar el manual, garantizando que las políticas sean técnicamente adecuadas y operativamente aplicables. Asimismo, se habilitará un repositorio digital protegido para centralizar documentos, versiones y evidencias.

Fase de diseño del manual

El manual se construirá por capítulos, incorporando: política general de seguridad, control de accesos, uso aceptable de recursos, protección de datos, respaldo y recuperación, seguridad de red y estaciones de trabajo, gestión de incidentes y continuidad operativa. Cada capítulo deberá incluir objetivo, alcance, reglas operativas claras, requisitos mínimos de configuración, responsables por rol y referencia a controles pertinentes de la norma ISO/IEC 27001:2022.

Validación técnica

El manual será revisado por el responsable técnico para asegurar coherencia, control real del riesgo y viabilidad con la infraestructura actual. Esta validación se enfocará en eliminar ambigüedades, garantizar que cada regla sea ejecutable y verificar que los controles propuestos reduzcan efectivamente la exposición.

Validación organizacional

La dirección del estudio verificará que el manual no afecte el cumplimiento contable y tributario, que sea realizable con los recursos disponibles y que no contradiga obligaciones contractuales o legales. Esta validación permitirá ajustar exigencias a la realidad operativa sin perder el objetivo de protección.

Socialización y capacitación

El estudio desarrollará jornadas breves de capacitación interna para asegurar comprensión y adopción. Se priorizará la explicación práctica de reglas clave (contraseñas, acceso a archivos, uso de almacenamiento en la nube, control de memorias externas, respaldos y

reporte de incidentes). Además, se establecerá un mecanismo de confirmación de entendimiento mediante listas de asistencia o formatos internos.

Etapa 4: Recomendaciones para una implementación gradual

La propuesta reconoce que el estudio contable no puede implementar todos los controles al mismo tiempo sin afectar la operación. Por ello, se plantea una implementación por fases, priorizando controles críticos y avanzando hacia madurez progresiva.

Fase 1: Seguridad fundamental (primer mes)

El estudio implementará controles mínimos inmediatos: eliminación de cuentas compartidas, fortalecimiento de credenciales, configuración segura de red inalámbrica, revisión y aseguramiento de respaldos operativos con prueba de restauración, y organización básica de carpetas con permisos diferenciados según rol. Esta fase busca reducir rápidamente riesgos de fuga de información y pérdida operativa.

Fase 2: Procedimientos formales (segundo al tercer mes)

Se formalizarán prácticas mediante reglas internas: política de contraseñas, normas de uso aceptable, control del uso de memorias externas, uso seguro del almacenamiento en la nube y capacitación orientada a manejo responsable de información. Además, se implementará un registro simple de incidentes para iniciar trazabilidad y aprendizaje.

Fase 3: Madurez y automatización (cuarto mes en adelante)

Se fortalecerán controles mediante automatización y seguimiento: automatización de copias de seguridad cuando sea viable, monitoreo básico de eventos relevantes, pruebas periódicas de restauración con evidencias y ajustes en infraestructura según brechas persistentes (por ejemplo, mejora de segmentación de red o fortalecimiento de controles en estaciones de trabajo).

Fase 4: Cultura de seguridad y mejora continua

La propuesta enfatiza que el objetivo final será instalar una cultura de seguridad sostenida. Para ello, el estudio revisará periódicamente el nivel de cumplimiento utilizando la misma lista de cotejo, medirá mejoras y ajustará controles. La seguridad será asumida como responsabilidad compartida, donde el personal comprende su rol en la protección de

información de clientes, y donde los incidentes se convierten en oportunidades de mejora, no en prácticas ocultas.

Limitaciones de la propuesta

El presente proyecto no desarrolla políticas formales ni implementa controles de seguridad. Su alcance se limita a la elaboración de lineamientos conceptuales y a la formulación de una ruta referencial basada en los resultados del diagnóstico. La elaboración del manual, su aprobación, validación e implementación corresponden exclusivamente al estudio contable JC TICONA en una etapa posterior.

5.4. Presupuesto

Tabla 23
Presupuesto estimado del proyecto

Concepto	Descripción	Costo estimado (S/)
Consultoría especializada en seguridad de la información	Servicio brindado por un consultor externo en seguridad de la información, con experiencia en ISO/IEC 27001:2022, para asesorar el diseño del manual de políticas sobre la base de los lineamientos conceptuales formulados en este proyecto.	S/. 1,200
Revisión técnica y validación externa	Evaluación del borrador del manual por un especialista independiente en seguridad de la información o por una empresa consultora en ciberseguridad, a fin de verificar su coherencia técnica, pertinencia y alineación con la ISO/IEC 27001:2022.	S/. 500
Capacitación introductoria	Sesión inicial de sensibilización dirigida por un capacitador o consultor en seguridad de la información para socializar el contenido del manual y orientar su aplicación básica dentro del estudio contable.	S/. 350
Edición e impresión del manual	Edición e impresión de 4 copias de la versión final aprobada.	S/. 250
Total estimado		S/. 2,300

Nota: Elaboración propia

El presupuesto estimado asciende a S/ 2,300 y se considera viable para el estudio contable JC TICONA, en tanto corresponde a una fase futura destinada al diseño, validación y difusión interna del manual de políticas de seguridad de la información. La mayor parte de

la inversión se orienta a la contratación de consultoría especializada y a actividades de socialización y validación, lo que refleja el enfoque estratégico y organizacional de la propuesta. Este presupuesto no forma parte del alcance operativo del presente proyecto, cuyo aporte se centra en el diagnóstico y en la definición de lineamientos conceptuales.

6. CONCLUSIONES Y RECOMENDACIONES

6.1. Conclusiones

En relación con el primer objetivo específico, se concluye que el estudio contable JC TICONA no cuenta con políticas formales, procedimientos documentados ni mecanismos suficientemente estructurados para regular el acceso, uso y almacenamiento de la información. Las prácticas observadas se desarrollan principalmente de manera empírica, sin respaldo normativo institucional, lo que se evidencia en la ausencia de una política general aprobada y comunicada, en la falta de un inventario formal de activos y en la inexistencia de criterios de clasificación y etiquetado de la información según su nivel de confidencialidad.

Respecto del segundo objetivo específico, se concluye que la ausencia o insuficiencia de controles y políticas de seguridad de la información expone al estudio a riesgos operativos, normativos y tecnológicos que pueden comprometer la confidencialidad, integridad y disponibilidad de los datos contables, tributarios y administrativos. Entre las principales brechas identificadas destacan la debilidad en los controles de acceso, la falta de clasificación de la información, la inexistencia de gestión formal de incidentes, el uso de canales informales para el intercambio de archivos y la insuficiente formalización de medidas de respaldo, lo que incrementa la vulnerabilidad institucional frente a pérdidas, accesos indebidos o alteraciones no autorizadas.

En atención al tercer objetivo específico, se concluye que el estudio permite formular lineamientos conceptuales para el futuro diseño de políticas de seguridad de la información adaptadas al contexto organizacional del estudio contable JC TICONA. Dichos lineamientos se orientan principalmente al control de accesos, la protección de datos, el respaldo y recuperación de información, la gestión de incidentes y la continuidad operativa, constituyéndose en una base técnica y organizacional para la futura elaboración de un manual formal de políticas, sin que ello implique aún la implementación de un sistema completo de gestión de seguridad de la información.

6.2. Recomendaciones

Se recomienda que el estudio contable JC TICONA formalice, como primera prioridad, una política general de seguridad de la información y los procedimientos básicos asociados al acceso, uso y almacenamiento de información sensible. Asimismo, debe elaborar un inventario actualizado de activos de información, definir roles y responsabilidades, e implementar criterios de clasificación y etiquetado, a fin de establecer una base documental mínima que permita ordenar y proteger adecuadamente los recursos informativos de la organización.

Se recomienda fortalecer la gestión de riesgos mediante la implementación progresiva de controles técnicos y operativos esenciales, tales como procedimientos documentados de control de accesos, mecanismos de respaldo y restauración, monitoreo de eventos de seguridad, regulación del uso de dispositivos externos y canales de intercambio de información, así como acciones básicas de capacitación y concientización del personal. Estas medidas permitirán reducir la dependencia de prácticas informales y mejorar la capacidad de prevención y respuesta ante incidentes de seguridad.

Se recomienda utilizar los lineamientos conceptuales formulados en la propuesta como base para la elaboración futura de un manual de políticas de seguridad de la información, priorizando los dominios de control de accesos, protección de datos, respaldo y recuperación, gestión de incidentes y continuidad operativa. Esta implementación debería realizarse de manera gradual, de acuerdo con las brechas identificadas, los recursos disponibles y las necesidades reales del estudio, con el fin de asegurar viabilidad técnica, sostenibilidad operativa y mejora progresiva en la protección de la información institucional.

7. REFERENCIAS BIBLIOGRAFICAS

Agencia Española de Protección de Datos. (2020). Guía de protección de datos por defecto. URL https://www.aepd.es/guias/guia-proteccion-datos-por-defecto.pdf

Asqui, J., y Torres, J. (2023). ISO 27001 para mejorar la seguridad de la información en una institución educativa, Lima 2022 (Tesis de pregrado, Universidad Norbert Wiener). https://repositorio.uwiener.edu.pe/entities/publication/77c76130-79ea-493c-8aa9-831761742808

Centro Criptológico Nacional. (2025). Guía de Seguridad de las TIC. CCN-STIC 801: Esquema Nacional de Seguridad – Responsabilidades y funciones. URL https://www.ccn-cert.cni.es/es/pdf/guias/series-ccn-stic/800-guia-esquema-nacional-de-seguridad/501-ccn-stic-801-responsibilidades-y-funciones-en-el-ens/file.html

Contador, J. y Tapia, C. (2024) Diseño e implementación de la ISO 27001 para mejorar la seguridad de información de la Empresa Minera Colibri S.A.C. Lima - 2023 (Tesis de pregrado, Universidad Nacional José Faustino Sánchez Carrión). https://repositorio.unjfsc.edu.pe/handle/20.500.14067/8975

Defensoría del Pueblo. (2023). La ciberdelincuencia en el Perú: Estrategias y retos del Estado (Informe Defensorial N.º 001-2023-DP/ADHPD). URL https://www.defensoria.gob.pe/wp-content/uploads/2023/05/ConsolidadoIA2022.pdf

Guarneros, L. (2023) Implementación de políticas de seguridad de información basadas en ISO 27001 (Tesis de maestría, Tecnológico de Estudios Superiores de Cuautitlán Izcalli). https://rinacional.tecnm.mx/handle/TecNM/6163

Lagos, J. (2024). Transformación digital y ciberseguridad (Tesis de doctorado, Universidad de Chile). https://repositorio.uchile.cl/handle/2250/205366

Ministerio de la Producción. (2023). Madurez digital en las empresas peruanas: Análisis de características y brechas para la transformación digital. URL

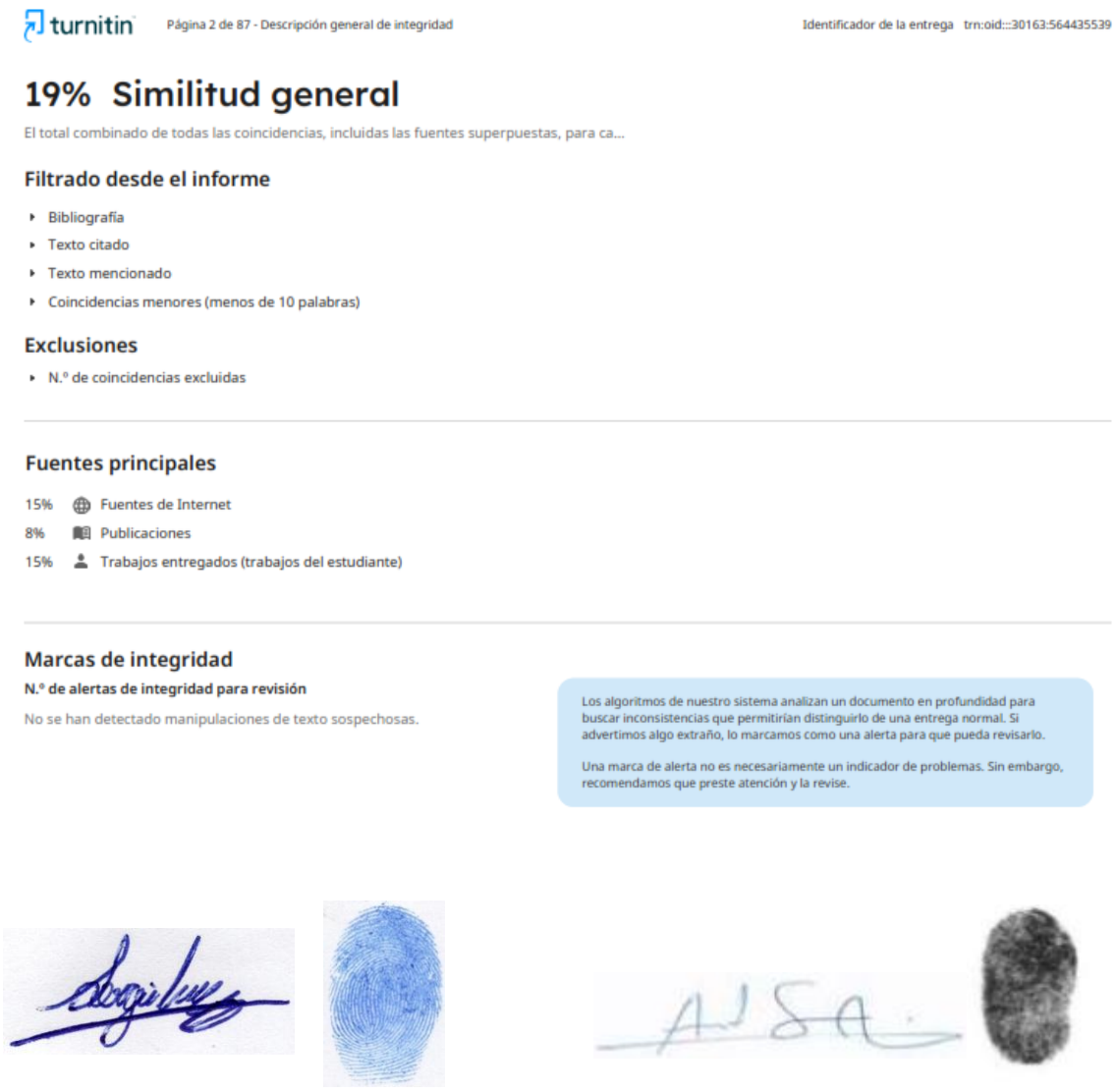
https://www.gob.pe/institucion/produce/informes-publicaciones/4954834-estudio-de-la-madurez-digital-en-las-empresas-peruanas

Ortiz, V. (2021). Diseño de las políticas de seguridad de la información en la Compañía de Seguros S.A. (Trabajo de pregrado, Universidad Católica de Colombia). https://repository.ucatolica.edu.co/entities/publication/9ff34551-fcce-4d4d-902a-d7237f8b5b46

Ticona, H. (2021). Uso de la norma ISO 27001 y su influencia en la seguridad de información de la empresa ICO el año 2021 (Tesis de pregrado, Universidad Privada del Norte). https://repositorio.upn.edu.pe/item/1038c21c-2e02-441f-9410-8f99ca56d186

8. ANEXOS

8.1. Informe Turnitin



turnitin Página 2 de 87 - Descripción general de integridad Identificador de la entrega trn:oid:::30163:564435539

19% Similitud general

El total combinado de todas las coincidencias, incluidas las fuentes superpuestas, para ca...

Filtrado desde el informe

- Bibliografía
- Texto citado
- Texto mencionado
- Coincidencias menores (menos de 10 palabras)

Exclusiones

- N.º de coincidencias excluidas

Fuentes principales

15% Fuentes de Internet
8% Publicaciones
15% Trabajos entregados (trabajos del estudiante)

Marcas de integridad

N.º de alertas de integridad para revisión

No se han detectado manipulaciones de texto sospechosas.

Los algoritmos de nuestro sistema analizan un documento en profundidad para buscar inconsistencias que permitirían distinguirlo de una entrega normal. Si advertimos algo extraño, lo marcamos como una alerta para que pueda revisarlo.

Una marca de alerta no es necesariamente un indicador de problemas. Sin embargo, recomendamos que preste atención y la revise.

Sergio Juan, Luna cutipa (Autor)

Sam Anlas, Carlos Antonio (Asesor)

8.2. Registro de impacto y resultados

Tipo de documento: Trabajo de investigación

Título del Trabajo de Investigación o Tesis

"Propuesta de diseño de políticas de seguridad de la información en el estudio contable JC TICONA"

Integrante:

Luna Cutipa, Sergio Juan

Asesor:

Sam Anlas, Carlos Antonio

Impacto de la investigación

El impacto de una investigación se refiere a los efectos, tanto esperados como inesperados, que esta puede generar, abarcando aspectos económicos, políticos, culturales, ambientales, tecnológicos, sociales, entre otros.

La presente investigación genera un impacto tecnológico y organizacional, porque permite diagnosticar el nivel de cumplimiento de los controles de seguridad de la información en el estudio contable JC TICONA y, a partir de ello, formular lineamientos conceptuales para el futuro diseño de políticas alineadas con la ISO/IEC 27001:2022. Su aporte principal consiste en fortalecer la protección de activos de información sensibles, optimizar la gestión del acceso, uso, respaldo y almacenamiento de datos, y orientar la formalización de procedimientos internos sin requerir la implementación inmediata de un Sistema de Gestión de Seguridad de la Información.
Asimismo, el estudio presenta un impacto económico y social, ya que contribuye a reducir riesgos asociados a pérdida de información, accesos no autorizados, interrupciones operativas y afectación de la confianza de los clientes. En ese sentido, la propuesta favorece la continuidad operativa, mejora la confiabilidad de los servicios contables y promueve una cultura organizacional orientada a la ciberseguridad, la resiliencia digital y la competitividad de la organización en un entorno de creciente exposición a amenazas tecnológicas.

Resultado del proceso de investigación

Los resultados de un proyecto de investigación son los descubrimientos o conclusiones alcanzadas después de realizar el estudio. Estos reflejan los datos obtenidos durante el proceso investigativo y responden a las preguntas o hipótesis formuladas al comienzo del proyecto. Los resultados son fundamentales para evaluar, interpretar y comprender los efectos o la validez de lo investigado.

Como resultado del proceso de investigación, se identificó que el estudio contable JC TICONA presenta un nivel insuficiente de formalización en seguridad de la información, evidenciado en la ausencia de políticas documentadas, procedimientos estructurados y controles plenamente implementados. El análisis global de los 18 ítems evaluados mostró que 0 % se ubica en la categoría “Cumple”, 88.9 % en “Parcialmente cumple” y 11.1 % en “No cumple”, destacándose brechas críticas en la clasificación de la información y en la gestión del inventario de activos. Estos hallazgos confirmaron la existencia de riesgos y vulnerabilidades que afectan la confidencialidad, integridad y disponibilidad de la información institucional.

En función de estos resultados, la investigación permitió formular lineamientos conceptuales y una ruta referencial para el futuro diseño de políticas de seguridad de la información adaptadas a la realidad del estudio contable JC TICONA. Entre los principales resultados esperados y obtenidos se encuentran la identificación de brechas y riesgos críticos, la definición de componentes mínimos que deberán integrar futuras políticas formales —como control de accesos, uso aceptable, respaldo y recuperación de datos, gestión de incidentes y continuidad operativa— y la generación de una base técnica para la posterior elaboración y validación interna de un manual de políticas.

8.3. Matriz de consistencia

Problema	Objetivos	Método	Instrumento	Dimensiones, Dominio
Problema general	**Objetivo general**	Enfoque: - Cuantitativo Tipo de investigación: - Aplicada Diseño de investigación: - No experimental de corte transversal	Lista de cotejo, elaborada a partir de los requisitos de la norma ISO/IEC 27001:2022.	DIMENSIÓN 1: • Existencia de políticas documentadas • Roles y responsabilidades de seguridad • Inventario de activos • Uso y protección de la información • Clasificación y etiquetado de la información • Procedimientos de acceso a la información DIMENSIÓN 2: • Identificación de vulnerabilidades • Controles de respaldo • Control de accesos • Protección contra vulnerabilidades • Registro de incidentes • Capacitación en riesgos DIMENSIÓN 3: • Procedimientos mínimos establecidos • Controles esenciales implementados • Gestión de activos de información • Responsable de seguridad • Prácticas de mejora continua • Continuidad operativa
¿Qué elementos deben identificarse para formular una propuesta de políticas de seguridad de la información alineadas con la norma ISO/IEC 27001:2022 en el Estudio Contable JC TICONA?	Formular una propuesta de políticas de seguridad de la información alineadas con la ISO/IEC 27001:2022 para el Estudio Contable JC TICONA.			
Problemas específicos	**Objetivos específicos**			
P1: ¿Qué políticas, normas o procedimientos relacionados con el acceso, uso y almacenamiento de información confidencial existen actualmente en el Estudio Contable JC TICONA?	OE1: Identificar las políticas, normas o procedimientos existentes relacionados con el acceso, uso y almacenamiento de información confidencial en el Estudio Contable JC TICONA.			
P2: ¿Qué riesgos y vulnerabilidades se identifican en el Estudio Contable JC TICONA debido a la ausencia o insuficiencia de políticas de seguridad de la información??	OE2: Describir los riesgos y vulnerabilidades presentes debido a la ausencia o insuficiencia de políticas de seguridad de la información.			
P3: ¿Qué lineamientos mínimos deben considerarse para formular lineamientos conceptuales para el futuro diseño de políticas de seguridad de la información acordes con la realidad organizacional del Estudio Contable JC TICONA?	OE3: Determinar los lineamientos mínimos necesarios para el diseño de políticas de seguridad de la información adaptadas a la realidad del Estudio Contable JC TICONA.			

8.4. Instrumento de recolección datos

LISTA DE COTEJO

Evaluación del cumplimiento de controles de seguridad de la información en el estudio contable JC TICONA

Objetivo: Verificar el nivel de cumplimiento de los controles y prácticas de seguridad de la información en el estudio contable JC TICONA, de acuerdo con los lineamientos de la ISO/IEC 27001:2022.

Instrucciones: Marque con una **X** la categoría que corresponda según la evidencia observada en cada ítem de evaluación. Considere la siguiente escala:

- **C = Cumple:** existe evidencia formal, verificable y aplicada.
- **PC = Parcialmente cumple:** existe evidencia incompleta, informal o aplicada de manera no sistemática.
- **NC = No cumple:** no existe evidencia o el control no se aplica.

N.º	Ítem de evaluación	Valor		
		C	PC	NC
1	Existe una **política general de seguridad de la información** aprobada y comunicada.			
2	Se han definido **roles y responsabilidades** de seguridad de la información.			
3	La organización posee **inventario de activos de información** actualizado.			
4	Se aplican **reglas de uso aceptable de la información** y los recursos informáticos.			
5	La información se **clasifica y etiqueta** según su nivel de confidencialidad.			
6	Existen **procedimientos documentados** para el control de accesos.			
7	Se realiza **análisis o evaluación periódica de riesgos** de seguridad de la información.			
8	Se cuenta con medidas de **respaldo y restauración** de información.			
9	Existen mecanismos de **control de accesos físicos y lógicos** a equipos y archivos.			
10	Se aplican **medidas de protección contra malware** y vulnerabilidades técnicas.			
11	Se dispone de **mecanismos de monitoreo o registro de eventos** de seguridad.			
12	El personal recibe **capacitación y concientización** sobre seguridad de la información.			
13	Se planifica la **gestión de incidentes de seguridad** (detección, respuesta, registro).			
14	Se prevén acciones para **aprender de los incidentes y mejorar controles**.			
15	Existen medidas para la **protección de datos personales y confidenciales**.			
16	Se incluyen disposiciones sobre **uso de dispositivos personales y trabajo remoto**.			
17	Se definen **políticas de copia de seguridad y eliminación segura de información**.			
18	Se contempla la **continuidad del negocio** ante incidentes o interrupciones.			

Nota: Adaptado de la norma ISO/IEC 27001:2022(E), Anexo A, los controles de seguridad de la información descritos en la Tabla A.1 se derivan de manera directa y se alinean con los establecidos en la ISO/IEC 27002:2022.

8.5. Validación de expertos

Informe de juicio de expertos del instrumento de recolección de datos

I. DATOS

1.1. Nombre y apellido del docente: Mg. CARLOS ANTONIO SAM ANLAS
1.2. Cargo e institución del experto: DOCENTE ISIL
1.3. Nombre del instrumento: Lista de cotejo.
1.4. Autor del instrumento: Sergio Juan Luna Cutipa
1.5. Título de la investigación: Propuesta de diseño de políticas de seguridad de la información en el estudio contable JC TICONA.

II. ASPECTOS DE VALIDACIÓN:

CRITERIOS	INDICADORES	Deficiente 00-20%	Regular 21-40%	Buena 41-60%	Muy buena 61-80%	Excelente 81-100%
1. CLARIDAD	El ítem está redactado con un lenguaje preciso, comprensible y adecuado al nivel del encuestado.					X
2. OBJETIVIDAD	El ítem expresa conductas observables, medibles y no ambiguas.					X
3. ACTUALIDAD	El contenido es pertinente y se encuentra alineado con los avances actuales en ciencia y					X
4. ORGANIZACIÓN	La secuencia de los ítems responde a una lógica interna clara y coherente.					X
5. SUFICIENCIA	El número de ítems cubre de forma adecuada la totalidad de dimensiones e indicadores definidos.					X
6. INTENCIONALIDAD	Cada ítem está formulado con un propósito claro que permite evaluar los aspectos clave de la					X
7. CONSISTENCIA	Los ítems se fundamentan en teorías o evidencias científicas pertinentes y					X
8. COHERENCIA	Existe relación directa y lógica entre las dimensiones, indicadores e ítems.					X
9. METODOLOGÍA	El instrumento responde al enfoque, tipo y diseño metodológico planteado					X
10. PERTINENCIA	El instrumento es útil y funcional para recolectar los datos necesarios de acuerdo con los objetivos					X
PROMEDIO DE VALIDACIÓN						82%

III. PERTINENCIA DE LOS ÍTEMS O REACTIVOS DEL INSTRUMENTO

IV. PROMEDIO DE VALORACIÓN: 82%

V. OPINIÓN DE APLICABILIDAD:

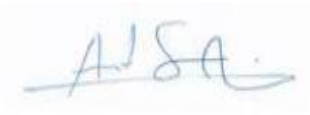
(X) El instrumento puede ser aplicado, tal como está elaborado.

( ) El instrumento debe ser mejorado antes de ser aplicado.

Mg. Carlos Antonio Sam Anlas

ORCID: 0000-0003-1632-7131

Escuela ISIL – Docente



FIRMA

HUELLA