UNIVERSIDAD TECNOLÓGICA ISRAEL

ESCUELA DE POSGRADOS "ESPOG"

MAESTRÍA EN SEGURIDAD INFORMÁTICA

Resolución: RPC-SO-02-No.053-2021.

PROYECTO DE TITULACIÓN EN OPCIÓN AL GRADO DE MAGISTER

Título del proyecto:
"GUÍA PARA LA IMPLEMENTACIÓN DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN SEGÚN LA NORMA ISO/IEC 27001 PARA LA INFRAESTRUCTURA Y EQUIPAMIENTO DE LA EMPRESA CORBANTRADE S.A.S."
Línea de Investigación:
Ciencias de la ingeniería aplicadas a la producción, sociedad y desarrollo sustentable
Campo amplio de conocimiento:
Tecnologías de la Información y la Comunicación (TIC)
Autor/a:
Juan Carlos Cumbicus Bravo
Tutor/a:
PhD. Toasa Guachi Renato Mauricio PhD. Urdaneta Herrera Maryory

Quito – Ecuador

2025

APROBACIÓN DEL TUTOR

Yo, Toasa Guachi Renato Mauricio con C.I: 1804724167 en mi calidad de Tutor del proyecto de investigación titulado: “Guía para la implementación de políticas de seguridad de la información según la norma ISO/IEC 27001 para la infraestructura y equipamiento de la empresa Corbantrade S.A.S”.

Elaborado por: Juan Carlos Cumbicus Bravo, de C.I: 1104020522, estudiante de la Maestría: Seguridad Informática, de la **UNIVERSIDAD TECNOLÓGICA ISRAEL (UISRAEL)**, como parte de los requisitos sustanciales con fines de obtener el Título de Magister, me permito declarar que luego de haber orientado, analizado y revisado el trabajo de titulación, lo apruebo en todas sus partes.

Quito D.M., Septiembre de 2025

Firmado electrónicamente por:
RENATO MAURICIO
TOASA GUACHI
Validar únicamente con FirmaEC

Firma

APROBACIÓN DEL TUTOR

Yo, Urdaneta Herrera Maryory con C.I: 1759316126 en mi calidad de Tutor del proyecto de investigación titulado: "Guía para la implementación de políticas de seguridad de la información según la norma ISO/IEC 27001 para la infraestructura y equipamiento de la empresa Corbantrade S.A.S.".

Elaborado por: Juan Carlos Cumbicus Bravo, de C.I: 1104020522, estudiante de la Maestría: Seguridad Informática, de la **UNIVERSIDAD TECNOLÓGICA ISRAEL (UISRAEL)**, como parte de los requisitos sustanciales con fines de obtener el Título de Magister, me permito declarar que luego de haber orientado, analizado y revisado el trabajo de titulación, lo apruebo en todas sus partes.

Quito D.M., Septiembre de 2025

MARYORY URDANETA HERRERA

Firmado digitalmente por MARYORY URDANETA HERRERA
Fecha: 2025.09.04 13:53:16 -05'00'

Firma

DECLARACIÓN DE AUTORIZACIÓN POR PARTE DEL ESTUDIANTE

Yo, Juan Carlos Cumbicus Bravo con C.I: 1104020522, autor/a del proyecto de titulación denominado: “Guía para la implementación de políticas de seguridad de la información según la norma ISO/IEC 27001 para la infraestructura y equipamiento de la empresa Corbantrade S.A.S.”. Previo a la obtención del título de Magister en Seguridad Informática.

1. Declaro tener pleno conocimiento de la obligación que tienen las instituciones de educación superior, de conformidad con el Artículo 144 de la Ley Orgánica de Educación Superior, de entregar el respectivo trabajo de titulación para que sea integrado al Sistema Nacional de Información de la Educación Superior del Ecuador para su difusión pública respetando los derechos de autor.
2. Manifiesto mi voluntad de ceder a la Universidad Tecnológica Israel los derechos patrimoniales consagrados en la Ley de Propiedad Intelectual del Ecuador, artículos 4, 5 y 6, en calidad de autor@ del trabajo de titulación, quedando la Universidad facultada para ejercer plenamente los derechos cedidos anteriormente. En concordancia suscribo este documento en el momento que hago entrega del trabajo final en formato impreso y digital como parte del acervo bibliográfico de la Universidad Tecnológica Israel.
3. Autorizo a la SENESCYT a tener una copia del referido trabajo de titulación, con el propósito de generar un repositorio que democratice la información, respetando las políticas de prosperidad intelectual vigentes.

Quito D.M., septiembre de 2025

Firmado electrónicamente por:
JUAN CARLOS CUMBICUS BRAVO
Validar únicamente con FirmaEC

_____

Firma

Tabla de contenidos

Índice de tablas

Índice de figuras

INFORMACIÓN GENERAL

Contextualización del tema

Según Romero (2024), para asegurar la continuidad de negocio, el cumplimiento normativo y aumentar la confianza del consumidor en el entorno empresarial actual, cada vez más digitalizado, la protección de la información es un elemento estratégico y de primer orden. La empresa ecuatoriana Corbantrade S.A.S., que ofrece servicios de asesoría contable y financiera, maneja información altamente sensible del día a día, como información de clientes y de la operación interna. Para prevenir accesos no autorizados, fugas o manipulaciones maliciosas de esta información, que incluye datos personales, registros contables y documentos financieros, se necesitan medidas de seguridad robustas.

Haciendo referencia a la *Política de Ciberseguridad (2021)*, a pesar de los avances tecnológicos que se han desarrollado en la infraestructura de Corbantrade S.A.S., no se cuentan con procedimientos definidos y estandarizados para la gestión de la seguridad de la información, en cumplimiento de estándares internacionales y normatividad local. Esta es una gran amenaza en cuanto a que se puedan generar incidentes de ciberseguridad, incumplimientos normativos por parte de la institución y daños a la marca de la institución.

Como lo indica Yagual (2024), en el contexto anterior, el objetivo de la investigación es proponer la creación de una guía práctica y metodológica para la aplicación de controles y mejores prácticas de seguridad de la información. Esta guía se apoyará en la norma ISO/IEC 27001:2022 y se adaptará a la LOPDP. La guía busca facilitar a Corbantrade S.A.S. una herramienta adaptable a su realidad operativa. La guía contendrá orientaciones técnicas, organizativas y jurídicas.

A través de esta guía la empresa podrá definir un marco de actuación en materia de seguridad de la información. Además, esta guía fortalecerá la cultura organizacional en materia de protección de datos y, por ende, mejorará la gestión de riesgos y la gestión de procesos tecnológicos y administrativos.

Problema de investigación

La seguridad de datos es un gran problema para las empresas actuales, sobre todo en sectores delicados como el contable o el financiero. Corbantrade S.A.S. se ha vuelto más susceptible a amenazas de seguridad, como accesos no autorizados, filtraciones de datos y fallas en los controles de acceso, a pesar de tener una infraestructura tecnológica.

No se ha establecido un sistema formal de normas de seguridad certificado bajo estándares como ISO/IEC 27001:2022 y la Ley Orgánica de Protección de Datos Personales (LOPDP) de

Ecuador para apoyar los objetivos de la empresa de incrementar el número de procesos que se digitalizan. Por falta de formalismo, se han abierto grandes agujeros. Estas vulnerabilidades abarcan desde software ilegal hasta falta de copias de seguridad confiables, pasando por conectar dispositivos personales a la red interna y una mala administración de información crítica.

Ante esta situación, es necesario disponer de una herramienta que permita a la organización implementar un programa de gestión conforme a ISO/IEC 27001:2022 y LOPDP. El objetivo es salvaguardar los activos tecnológicos y la información personal, reduciendo riesgos y asegurando el cumplimiento normativo.

Por lo tanto, el problema de esta investigación es la ausencia de una guía para Corbantrade S.A.S. para implementar políticas de seguridad de la información en sus riesgos tecnológicos, leyes y regulaciones, y proteger sus activos de información y datos personales.

Objetivo general

Elaborar una guía para la implementación de políticas de seguridad de la información en la empresa Corbantrade S.A.S., basada en la norma ISO/IEC 27001:2022 y alineada con la Ley Orgánica de Protección de Datos Personales.

Objetivos específicos

- Contextualizar los fundamentos teóricos y normativos relacionados con la seguridad de la información, tomando como base la norma ISO/IEC 27001:2022 y la Ley Orgánica de Protección de Datos Personales (LOPDP).
- Diagnosticar el estado actual de la seguridad de la información en Corbantrade S.A.S., identificando activos críticos, vulnerabilidades y riesgos asociados a la infraestructura tecnológica y a los datos personales.
- Diseñar una guía detallada que sirva de referencia para poner en práctica políticas de seguridad de la información, cumpliendo tanto la norma ISO/IEC 27001:2022 como la LOPDP.
- Validar la aplicabilidad y utilidad de la guía a través de revisión de especialistas y la retroalimentación técnica o prueba piloto dentro del entorno organizacional.

Vinculación con la sociedad y beneficiarios directos

El presente proyecto de titulación se orienta al desarrollo de una guía para la implementación de políticas de seguridad de la información, conforme a los lineamientos establecidos por la norma ISO/IEC 27001:2022 y la Ley Orgánica de Protección de Datos Personales (LOPDP). Esta

iniciativa establece un vínculo efectivo con la sociedad al ofrecer una herramienta práctica que contribuye al fortalecimiento del tratamiento adecuado de datos en entornos empresariales.

Como parte de las actividades de vinculación, se llevó a cabo una charla de socialización con el personal administrativo, contable, técnico y directivo de Corbantrade S.A.S., en la cual se presentaron los principales lineamientos de la guía y se explicaron buenas prácticas en materia de seguridad de la información y protección de datos personales. Esta actividad permitió sensibilizar a los colaboradores sobre la importancia de la ciberseguridad en su entorno laboral y fomentar una cultura organizacional más consciente respecto al manejo de la información.

Las evidencias de la charla y la participación del personal se presentan en los Anexos 5 al 9, lo que garantiza la transparencia del proceso de vinculación.

Igualmente, el concepto se vuelve más valioso socialmente en la medida en que puede ser replicado en otras PYMEs con problemas similares en el manejo de datos confidenciales. Esta herramienta es adaptable para usar en procesos internos de capacitación, así como en programas externos de capacitación y consultoría. Su arquitectura modular y su lenguaje técnico fácilmente comprensible la hacen excepcionalmente versátil.

El personal técnico, administrativo, contable y directivo de Corbantrade S.A.S. será el beneficiario directo de esta iniciativa. Se les proporcionarán normas claras para reforzar la gestión de la seguridad de la información y tomar decisiones informadas en materia de protección de datos. Como resultado, los clientes de la organización obtendrán beneficios indirectos, ya que se les proporcionarán mayores garantías en cuanto a la gestión adecuada y responsable de su información personal y financiera.

Por último, tanto desde el punto de vista académico como profesional, este proyecto contribuye al desarrollo de conocimientos prácticos en materia de seguridad de la información. También sirve como recurso de referencia para futuras investigaciones, publicaciones y procesos de formación centrados en la mejora de la cultura de la ciberseguridad en el sector empresarial ecuatoriano.

CAPÍTULO I: DESCRIPCIÓN DEL PROYECTO

1.1. Contextualización general del estado del arte

El conocimiento que posee una empresa es uno de los activos más valiosos que tiene en el entorno digital moderno. Debido a la naturaleza del entorno, se han desarrollado varias soluciones con el fin de mejorar la seguridad de los sistemas informáticos y proteger los datos que se gestionan dentro del entorno corporativo. El manejo diario de información financiera y personal confidencial requiere la formulación de procedimientos claros para garantizar la seguridad de la información frente a amenazas internas y externas. Esto es especialmente necesario en las empresas que operan en el sector contable, como Corbantrade S.A.S.

La ISO/IEC 27001:2022 es uno de los referentes más sólidos en la gestión de la seguridad de la información en todo el mundo. Esta norma contribuye un marco para establecer un Sistema de Gestión de Seguridad de la Información (SGSI) basado en la gestión de riesgos. Además, permite implementar controles administrativos, técnicos y físicos que protegen los activos de tecnología de la información. En su estudio práctico en una empresa de servicios, Aguilar y Cuenca (2025) manifiestan que la norma ISO/IEC 27001 refuerza la seguridad de la información y sobre todo crea una cultura de seguridad en toda la organización, que se alcanza integrando procesos, personas y tecnologías en un marco estandarizado y auditable.

Según Lema (2025), este método se basa en la propuesta de un modelo de seguridad para el sector de las telecomunicaciones, usando como base las normas ISO/IEC 27001 e ISO/IEC 27005. La aplicación de este enfoque permitió identificar de forma más precisa los riesgos y definir los activos más relevantes de la organización, lo que, finalmente, se tradujo en la mejora de la capacidad de la organización en cuanto a la prevención y la respuesta a los incidentes.

En cuanto al ámbito jurídico, la LOPDP, vigente en Ecuador desde 2021, obliga a las empresas a establecer mecanismos que aseguren el cumplimiento de los derechos de los titulares de datos. Catota (2025) afirma que la mayoría de las empresas en Ecuador no cuentan con la preparación necesaria para cumplir con la LOPDP. Esto se debe principalmente a la ausencia de una cultura que priorice la protección de la información personal. Utilizando una empresa fiduciaria como caso de estudio, llegó a la conclusión de que el establecimiento de un sistema de gestión de la seguridad de la información (SGSI) junto con los principios de la LOPDP puede ayudar a mitigar los riesgos legales y operativos asociados a la gestión inadecuada de los datos.

Tras llevar a cabo una investigación sobre la situación jurídica de las instituciones financieras ecuatorianas, Moscoso (2025) descubrió deficiencias sustanciales en la evaluación del riesgo

jurídico. El autor hace énfasis en que las empresas deben seguir ciertas normas legales como el permiso, la confidencialidad de los datos y la protección técnica que se da. Los resultados de su estudio revelan que muchas empresas desconocen las consecuencias legales de un tratamiento ilícito de datos. Esto crea la necesidad de soluciones que faciliten el cumplimiento normativo.

Verdugo (2023)) propone un modelo de madurez en ciberseguridad para Ecuador, ya que el país requiere adaptar los marcos internacionales a su contexto tecnológico, operativo y cultural. Este modelo se plantea desde la perspectiva de la madurez organizacional. De acuerdo a su investigación, gran parte de las empresas ecuatorianas son aún incipientes y carecen de controles o los tienen deficientes. Esto les impide defenderse de amenazas actuales como el ransomware, el phishing o las violaciones internas. En este contexto, propone desarrollar líneas guía realistas para poder ir implementando buenas prácticas, especialmente para las pequeñas y medianas empresas (pymes) que no tienen personal especializado en ciberseguridad.

El Marco de Ciberseguridad del NIST fue utilizado por Yánez (2022) en una institución educativa de Ecuador, quien presentó una propuesta muy similar a esta para su consideración. La investigación llega a la conclusión de que las recomendaciones adaptadas a las necesidades específicas de cada tipo de organización pueden ser más eficaces que la simple adopción de normas mundiales en su totalidad. Para que cualquier institución (en especial las que no tienen personal técnico muy capacitado) pueda controlar sus riesgos cibernéticos, se deben facilitar instrucciones comprensibles, contextualizadas y de fácil acceso al público al que van dirigidas.

Además, la Política Nacional de Ciberseguridad (2021), un documento gubernamental, ya hace un diagnóstico preocupante al señalar que muchas pequeñas y medianas empresas (PYMES) en Ecuador no tienen un plan de ciberseguridad tradicional. En el informe se sostiene que, para fortalecer la preparación de las instituciones, el país requiere de instrumentos sectoriales específicos, sistemas de soporte técnico e instrucciones prácticas. En esta línea, se recomienda adoptar normas internacionales como la ISO/IEC 27001 y elaborar guías para facilitar la aplicación de estas normas a nivel nacional.

Mientras que Morocho (2025) encuentra una vulnerabilidad en el uso de medidas técnicas de protección de datos en su análisis del sistema nacional de rendición de cuentas. Esta debilidad sale a la luz gracias a las conclusiones de Morocho. Cuando se trata de responder de manera eficiente a posibles incidentes, solo un pequeño número de organizaciones ha creado procesos duraderos o políticas internas, a pesar de que muchas organizaciones reconocen la importancia de la seguridad de la información. A raíz de los resultados de su investigación, llegó a la conclusión de que la formulación de directrices con el objetivo de garantizar el cumplimiento

de la LOPDP, que se basarían en normas como la ISO/IEC 27001, podría ser un punto de partida adecuado para mejorar la situación actual.

En la misma línea, Nuñez (2025) propone una metodología para la administración de la seguridad de la información destinada a las cooperativas de crédito del Segmento 1. El trabajo que ha realizado ilustra que la adopción de un sistema de gestión de la seguridad de la información (SGSI) debe ir acompañada de actividades de formación y sensibilización adaptadas a la cultura y las capacidades de cada empresa. Su estrategia adopta un enfoque gradual, que permite a las empresas determinar su nivel actual, establecer sus prioridades y avanzar hacia la certificación o el cumplimiento normativo.

Existe un consenso generalizado entre todos estos estudios sobre la necesidad de traducir las normativas y estándares en materiales de asesoramiento que no solo sean comprensibles, sino también aplicables y reproducibles. No basta con contar con la norma ISO/IEC 27001 o la LOPDP para garantizar el cumplimiento; es necesario que exista una conexión entre la teoría y la práctica. Con este fin, el desarrollo de una guía para la implementación de políticas de seguridad de la información que estén alineadas con la LOPDP y basadas en la norma ISO/IEC 27001:2022 está totalmente justificado como solución a una necesidad que aún no se ha resuelto. Este proyecto ha recomendado la creación de dicha guía.

Una empresa que opera en el sector contable y financiero, Corbantrade S.A.S., se enfrenta actualmente a problemas específicos relacionados con la protección de su información y la de sus clientes. Se trata de un caso emblemático para muchas otras pequeñas y medianas empresas (pymes) de Ecuador, ya que no cuenta con procedimientos organizados, no dispone de formación interna y está ampliando su infraestructura tecnológica. Mediante esta guía se proporcionará a la organización un documento estratégico y operativo que orientará la implementación progresiva de medidas de seguridad, teniendo en cuenta tanto el cumplimiento normativo y la realidad técnica de la empresa, para guiar la implementación de medidas de seguridad.

Es por ello por lo que el propósito de este trabajo no es sólo mejorar la seguridad informática de Corbantrade S.A.S., sino servir como guía para otras organizaciones con características similares, impactando positivamente en el mundo empresarial, académico y social.

1.2. Proceso metodológico de la investigación

El propósito es desarrollar una guía para la implementación de políticas de seguridad de la información. Esta guía seguirá las recomendaciones de la norma ISO/IEC 27001:2022 y se

adaptará a la Ley Orgánica de Protección de Datos Personales (LOPDP). Esta guía se ha elaborado para adaptarse específicamente a las condiciones tecnológicas y operativas de la empresa Corbantrade S.A.S. Para ello se empleó un enfoque metodológico mixto. Esta mirada permitió integrar métodos cuantitativos y cualitativos de análisis, los que finalmente dieron como resultado una mirada comprensiva y situada del mundo que se estaba estudiando.

1.2.1. Población y muestra

La población del estudio estuvo compuesta por los 26 empleados de Corbantrade S.A.S., que representan la totalidad del personal administrativo, operativo y técnico involucrado en la gestión contable, financiera y en el manejo de información dentro de la organización. La muestra se definió mediante un muestreo no probabilístico de tipo intencional, seleccionando de manera deliberada a 11 trabajadores de distintas áreas, junto con dos informantes clave —uno del área de tecnología de la información y otro del área administrativa—, cuya experiencia resultaba fundamental para aportar criterios precisos sobre los procesos de seguridad aplicados en la empresa. Esta decisión metodológica se adoptó porque el objetivo de la investigación no era obtener resultados con validez estadística generalizable, sino profundizar en las percepciones, necesidades y prácticas relacionadas con la gestión integral de la seguridad de la información y la protección de los activos tecnológicos de Corbantrade S.A.S.

1.2.2. Instrumentos

Para la recopilación de datos, se utilizaron los siguientes instrumentos:

1.2.2.1. Encuesta estructurada

Aplicado a quienes trabajan en funciones administrativas y operativas. Con el fin de medir el nivel de conocimiento, percepción y prácticas en materia de seguridad de la información, cumplimiento normativo y protección de datos, se utilizaron preguntas cerradas que se calificaron en una escala Likert de cinco niveles.

1.2.2.2. Entrevista semiestructurada

Está dirigido a los miembros del personal de tecnología de la información, así como a los responsables administrativos, con el fin de investigar las cuestiones técnicas y organizativas relacionadas con la gestión de activos, los controles de acceso y las deficiencias en la formación del personal.

1.2.2.3. Revisión bibliográfica

Entre ellos se incluían materiales académicos, normas tanto internacionales como nacionales, trabajos de investigación previos y políticas actualmente en vigor en materia de ciberseguridad.

Las pruebas de los instrumentos utilizados comprenden el formato de la encuesta, el cuestionario y los guiones de las entrevistas, todos los cuales se encuentran en los anexos 1 a 4.

1.2.3. Método cuantitativo

Se entregó un cuestionario estructurado al personal administrativo y operativo de la organización con el fin de recopilar datos para el componente cuantitativo del estudio. El objetivo principal de este instrumento era determinar el nivel de familiaridad, percepción y prácticas del personal con respecto a la seguridad de la información y el cumplimiento de las normas legales. Se utilizó una escala Likert de cinco puntos, que es una herramienta excelente para determinar el grado en que las personas están de acuerdo o en desacuerdo con afirmaciones importantes relacionadas con el tema en cuestión.

Las preguntas incluidas en el cuestionario abarcaban diversos temas, entre ellos el nivel de familiaridad con la norma ISO/IEC 27001 y la LOPDP, la percepción de los riesgos de la tecnología de la información dentro de la organización, la existencia (o ausencia) de normas internas de seguridad, la aplicación de las mejores prácticas en la gestión de la información sensible y la evaluación por parte del personal de la necesidad de una guía técnica para facilitar la aplicación de los controles. En el anexo 1 se presenta el marco general de la encuesta, y en el anexo 2 se pueden consultar las preguntas que se formularon.

Mediante el uso de la encuesta, fue posible recopilar datos cuantitativos y objetivos, y se demostró el estado actual de la cultura organizativa con respecto a la seguridad de la información. A continuación, se procesaron y analizaron los resultados con el fin de determinar de manera más precisa los aspectos prioritarios que debían incluirse en la guía. Esto se hizo con el fin de garantizar que la guía fuera pertinente, funcional y acorde con las necesidades reales de la organización.

1.2.4. Método cualitativo

En el enfoque cualitativo se emplearon dos metodologías complementarias. Para capturar información de profesionales y directivos de TI con poder de decisión estratégica, se realizó una entrevista semiestructurada. Este enfoque hizo posible que se pudiera hacer una revisión más exhaustiva de las vulnerabilidades encontradas en dimensiones como la gestión de activos de TI, infraestructura tecnológica, control de acceso, identificación y tratamiento de riesgos, gestión de datos personales. En el anexo 3 (Administración) y en el anexo 4 (Sistemas) se adjuntan los guiones y formularios de las entrevistas realizadas. Puede consultarlos en los documentos adjuntos.

Además, se realizó una revisión bibliográfica exhaustiva de materiales académicos, tesis de grado anteriores, marcos legales existentes, políticas gubernamentales, normas técnicas internacionales. La norma ISO/IEC 27001:2022, la LOPDP, la Política Nacional de Ciberseguridad (2021), las actuales investigaciones sobre la adopción de SGSI en el tejido empresarial nacional son algunas de las fuentes que sobresalen entre las consultadas. Esta revisión hizo posible organizar la guía de forma teórica, pero que se ajuste a las normas mundialmente establecidas y a la realidad del contexto ecuatoriano.

1.2.5. Aplicación combinada del método mixto

El uso de métodos de investigación cuantitativos y cualitativos permitió la elaboración de una propuesta coherente y apoyada en evidencia técnica. La guía se organizó en módulos temáticos, desde los fundamentos teóricos y legales hasta las formas de implementación y las herramientas prácticas (plantillas, listas de verificación, etc.). Estas partes se estructuraron tras un análisis cruzado de los datos.

El propósito de este documento es brindar a empresas como Corbantrade S.A.S. que deseen mejorar su seguridad de la información, una herramienta no solo útil, sino también efectiva y adaptable. Después de analizar a fondo los resultados de la investigación, se validó conceptualmente la estructura de la guía.

En definitiva, la metodología utilizada en el proyecto permitió conocer en profundidad el entorno organizativo y legal y establecer las bases para desarrollar una herramienta práctica, realista y efectiva. Esta donación impacta no solo a Corbantrade S.A.S., sino que puede replicarse en otras pymes del sector contable y financiero, mejorando la cultura de protección de la información en Colombia.

1.3. Análisis de resultados

Gracias a los resultados del uso del método mixto, ahora conocemos cómo se encuentra la gestión de seguridad de la información en Corbantrade S.A.S. y lo que piensan, saben y hacen sus colaboradores en cuanto a cumplimiento normativo.

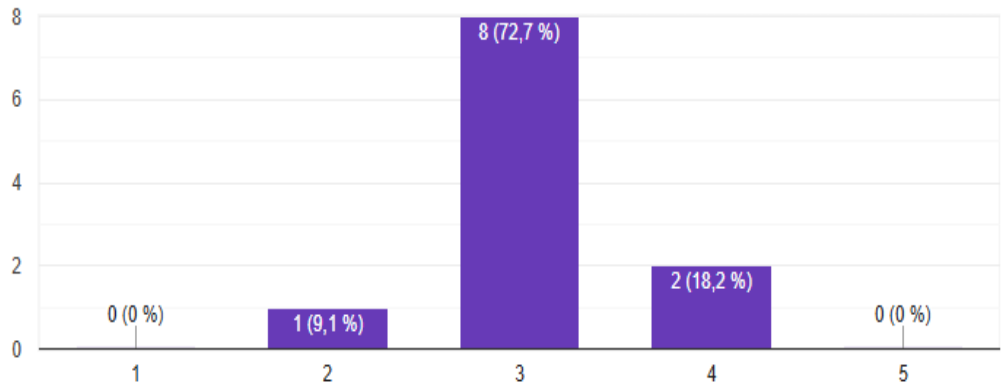
1.3.1. Análisis cuantitativo

La encuesta se elaboró con preguntas de opción múltiple tipo escala Likert de cinco puntos para medir las actitudes y opiniones de la plantilla. Las respuestas obtenidas fueron procesadas y graficadas a través de Google Forms. A continuación, se muestran los resultados de las preguntas clave con su interpretación. El formato de encuesta se lo puede evidenciar en los Anexos 1 y 2.

1. Conozco los principios generales de la norma ISO/IEC 27001.

Según los datos de la Figura 1, la mayoría de los encuestados (72,7 %) mostró un conocimiento limitado o superficial de los principios generales de la norma ISO/IEC 27001, mientras que solo un 18,2 % afirmó conocerlos. Estos resultados evidencian la necesidad de implementar procesos de formación continua que refuercen la comprensión del marco normativo en seguridad de la información, el cual es crucial para la protección y gestión de los activos informáticos.

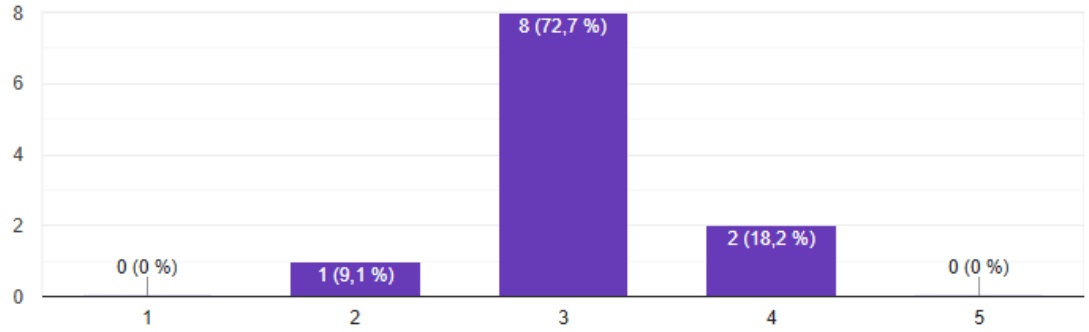
Figura 1
Conocimiento de los principios generales de la norma USO/IEC 27001.



2. Tengo noción de los derechos que establece la Ley Orgánica de Protección de Datos Personales (LOPDP).

Tal como se observa en la Figura 2, el 72,7 % del personal encuestado indicó tener un conocimiento limitado sobre los derechos establecidos por la Ley Orgánica de Protección de Datos Personales (LOPDP). Estos resultados proporcionan más pruebas de que la mayoría de los empleados necesitan formación adicional sobre sus derechos y obligaciones en materia de privacidad de datos, lo cual es un componente esencial para cumplir con la legislación vigente.

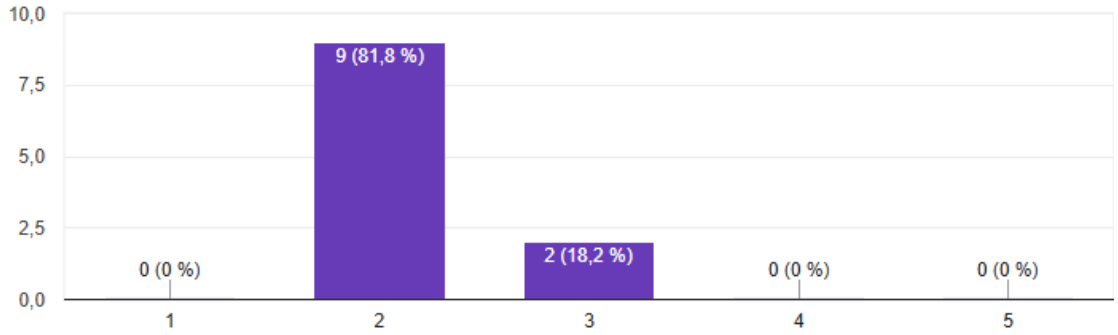
Figura 2
Comprensión de la LOPDP.



3. En la empresa existen políticas claras sobre el manejo de información confidencial.

Los datos que se muestran en la figura 3 demuestran que el 81,8 % de los participantes tenía la impresión de que la organización no contaba con políticas claras en materia de gestión de la información sensible. Esta falta de formalización y comunicación de las políticas internas pone en riesgo la capacidad de la organización de dar cumplimiento a certificaciones como ISO/IEC 27001 o LOPDP. Esto hace notar la importancia de crear y difundir normas claras sobre el tema.

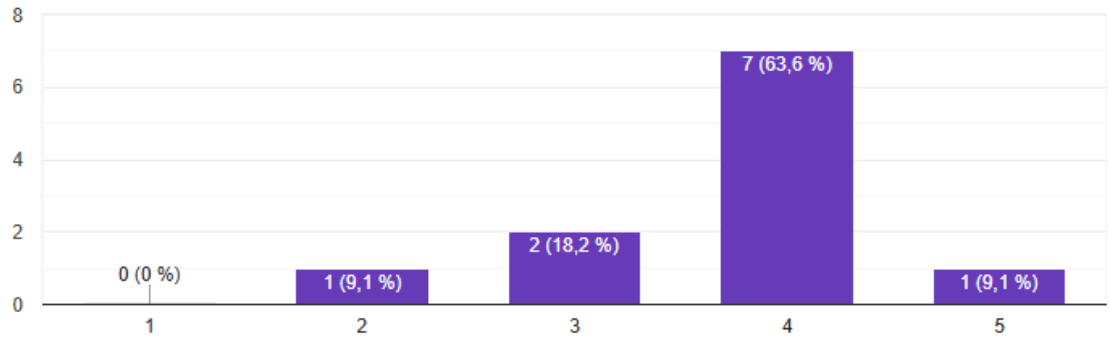
Figura 3
Políticas sobre información confidencial.



4. Se aplican buenas prácticas para el manejo de contraseñas y accesos.

Los resultados de la encuesta se muestran en la figura 4, donde el 63,6% de los encuestados considera que sí que existen buenas prácticas para la gestión de contraseñas y accesos. Aunque estos resultados muestran que hay una tendencia favorable en el uso de medidas básicas de seguridad, es preciso fortalecer estas prácticas con políticas escritas y procedimientos de sensibilización continua para que sean efectivas.

Figura 4
Prácticas relacionadas con contraseñas y accesos.

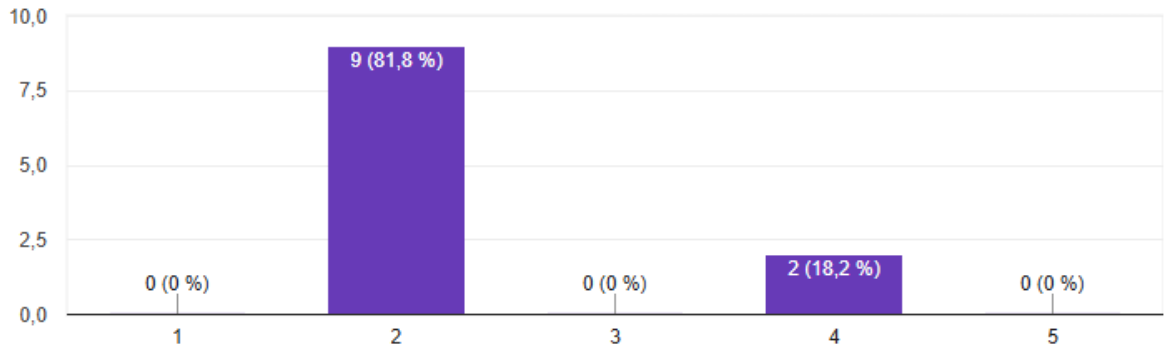


5. He recibido capacitación sobre seguridad de la información o protección de datos.

Como se puede observar en la figura 5, el 81,8 % de los miembros del personal afirmó haber recibido muy poca formación en materia de protección de datos y seguridad de la información.

Este resultado pone de manifiesto una grave deficiencia en el proceso de formación interna. Esta deficiencia limita la capacidad de los empleados para aplicar las mejores prácticas e identificar los riesgos. Por lo tanto, se recomienda implementar un plan de formación continuo y adaptado al contexto de la empresa.

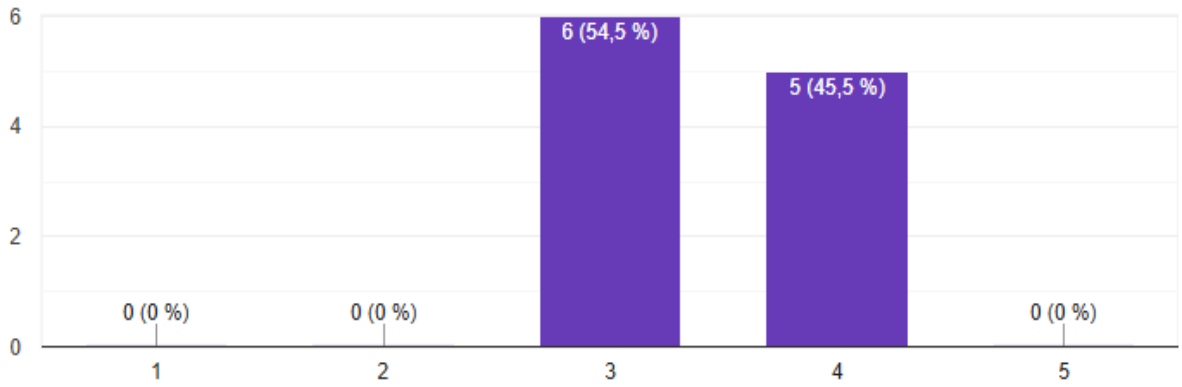
Figura 5
Capacitación recibida en seguridad.



6. Considero que los sistemas de respaldo de información están correctamente implementados.

En la Figura 6, se observa que el 54,5 % de los encuestados percibe que los sistemas de respaldo están medianamente bien implementados, sin mostrar una confianza plena. Este patrón de respuesta sugiere que, si bien existen mecanismos de respaldo, su implementación o conocimiento podrían ser insuficientes, lo que refuerza la necesidad de fortalecer la comunicación interna sobre los procedimientos y la eficacia de estos sistemas.

Figura 6
Percepción sobre respaldos de información.

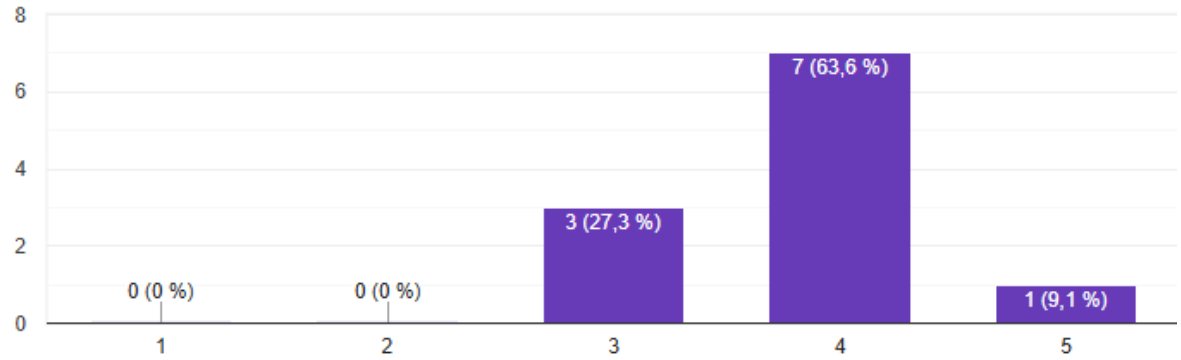


7. El acceso a los sistemas de la empresa está adecuadamente controlado.

La Figura 7 indica que la mayoría de los encuestados (63,6 %) considera que el acceso a los sistemas está adecuadamente controlado. Esta percepción positiva sugiere que, si bien los

mecanismos de control existen, podrían fortalecerse mediante documentación formal y auditorías regulares para garantizar su efectividad y continuidad.

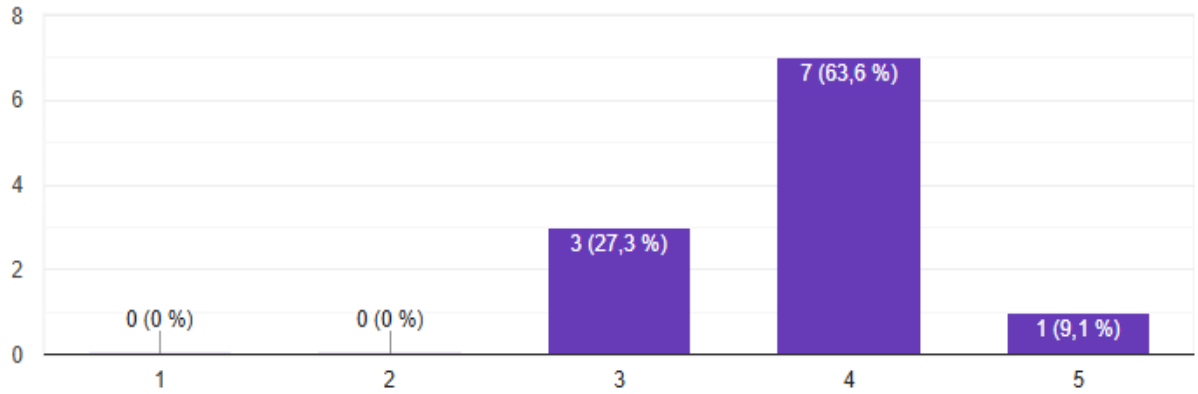
Figura 7
Control de accesos a los sistemas.



8. Uso buenas prácticas al manejar información sensible (clientes, finanzas, etc.).

La Figura 8 refleja que el 63,6 % de los encuestados percibe que aplica buenas prácticas en el manejo de información sensible. La ausencia de respuestas negativas sugiere una base de conciencia, aunque los resultados también indican oportunidades de mejora. Sería recomendable fortalecer este aspecto con capacitaciones periódicas y la formalización de políticas sobre el tratamiento adecuado de datos críticos.

Figura 8
Prácticas con información sensible.

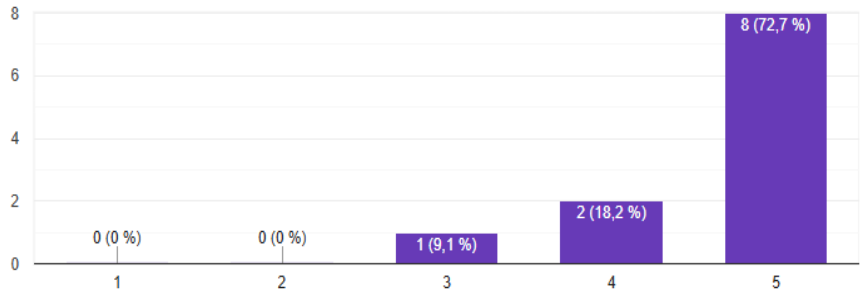


9. Me preocupa la posibilidad de incidentes de seguridad informática en la empresa.

Según la Figura 9, el 72,7 % de los encuestados manifestó una alta preocupación por la posibilidad de incidentes de seguridad informática. Esta percepción del riesgo puede utilizarse

para fomentar una cultura organizacional enfocada en la prevención y respuesta a incidentes, lo cual fortalecería las medidas de seguridad existentes.

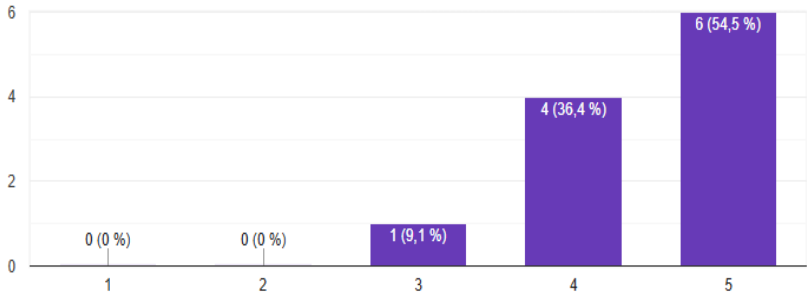
Figura 9
Preocupación por incidentes.



10. Considero útil contar con una guía práctica que ayude a mejorar la seguridad de la información en la empresa.

De acuerdo con la Figura 10, la mayoría de los participantes (90,9 %) indicó estar de acuerdo con la utilidad de contar con una guía práctica para mejorar la seguridad de la información. La importancia de desarrollar una herramienta para orientar las acciones del personal en materia de cumplimiento normativo y protección de datos queda validada por el alto nivel de aceptación que ha recibido dicha herramienta.

Figura 10
La utilidad de un manual práctico.



1.3.2. Análisis cualitativo

Se obtuvieron datos precisos y específicos sobre el estado actual de la seguridad de la información dentro de la empresa mediante entrevistas semiestructuradas con un representante del departamento de tecnología de la información y un funcionario administrativo.

El jefe del departamento técnico mencionó que la organización ha implementado algunas medidas de seguridad, como el uso de un firewall corporativo WatchGuard, el uso de redes de área local virtuales (VLAN) para la segmentación de la red y políticas básicas para la renovación

de contraseñas. Sin embargo, admitió que estos controles no están respaldados por políticas codificadas ni procedimientos establecidos. Afirmó que esto era aceptable.

También se encontró que las copias de seguridad de los datos se almacenan localmente y no se utiliza una solución en la nube ni se realizan revisiones periódicas para verificar la integridad de los datos. Además, el entrevistado comentó un caso reciente de phishing que evidenció fallos en la capacitación del personal y la necesidad de concienciar a los usuarios con más formación. Aunque estas áreas claves han sido identificadas, implementar las reformas ha sido complicado por falta de tiempo y recursos. Finalmente, creyó que una asesoría personalizada para la organización sería de gran ayuda para mejorar la seguridad interna de la empresa y cumplir con la normativa.

El área administrativa concluyó que hay desconocimiento generalizado sobre los procesos de protección de datos personales y manejo de información confidencial. La persona entrevistada afirmó que no existen normas específicas sobre cómo responder a incidentes de seguridad y que no ha recibido formación profesional en este ámbito concreto.

Además, admitió que una gran cantidad de documentos privados se manejan sin las garantías adecuadas y que el acceso a datos cruciales no siempre está prohibido. Por otro lado, se mostró abierto a la idea de establecer normas que faciliten a los empleados la aplicación de los procedimientos de seguridad adecuados. Esto es especialmente cierto si las directrices se ajustan a la normativa vigente y son fáciles de usar.

1.3.3. Interpretación

Los resultados de esta investigación arrojan luz sobre una situación muy común en las pequeñas y medianas empresas ecuatorianas. En estas empresas, las medidas de seguridad de la información suelen ser aisladas y no están respaldadas por una formación adecuada, políticas escritas o un conocimiento de la normativa vigente.

Esta situación hace necesario el desarrollo de este proyecto, el cual busca generar una guía para Corbantrade S.A.S. y así poder implementar políticas de seguridad de la información, dar cumplimiento a la norma ISO/IEC 27001:2022 y la Ley Orgánica de Protección de Datos Personales.

CAPÍTULO II: PROPUESTA

2.1. Fundamentos teóricos aplicados

La siguiente sección proporciona una descripción general de los conceptos clave que sustentan las directrices propuestas para establecer políticas de seguridad de la información. Estos conceptos teóricos son esenciales para entender el marco conceptual del proyecto, que abarca dimensiones tecnológicas, legales y organizativas.

2.1.1. Seguridad de la información

La confidencialidad, integridad y disponibilidad de la información son los tres pilares de la seguridad de la información. Dichos principios buscan impedir el acceso ilegítimo a los datos, mantener la información íntegra, exacta y sin modificaciones no autorizadas, y asegurar que esté disponible para los usuarios que la necesiten en el momento oportuno. De acuerdo con Aguilar y Cuenca (2025), estos elementos son las bases de un sistema de gestión de seguridad de la información (SGSI) que generan confianza en los procesos internos, disminuyen los riesgos operativos y salvaguardan la imagen institucional. Así mismo, Nuñez (2025) manifiesta que las normas ISO/IEC 27000 se basan en estos principios para desarrollar políticas, definir procedimientos y el establecimiento de controles técnicos y organizativos. De esta forma, se asegura la creación de un marco para proteger la información.

2.1.2. Las normas ISO/IEC 27001:2022 internacionales

Es la norma más empleada para establecer, implementar, mantener y mejorar un Sistema de Gestión de Seguridad de la Información (SGSI). Según Nuñez (2025), la norma además de abarcar aspectos técnicos, también es un marco de gestión integral que desde el inicio alinea la estrategia de negocio de la organización con sus metas de seguridad. El ciclo PDCA (Planificar, Hacer, Verificar, Actuar) constituye la base de su metodología y asegura que los controles se revisen y ajusten periódicamente para ajustarse a las variaciones en las condiciones. Además, Aguilar y Cuenca (2025) resaltan que la certificación ISO/IEC 27001 permite identificar vulnerabilidades y establecer planes de acción que aseguran que la organización cumpla con la legislación local, como la LOPDP.

Para la particularidad de este caso, la figura 11 muestra la relación de la norma ISO/IEC 27001 con otras normas de la familia ISO/IEC 27000. Estas normas abarcan la ISO/IEC 27000, ISO/IEC 27002 e ISO/IEC 27005, que apoyan la implementación y mejoran la gestión de la seguridad de la información. La norma es parte de la estructura de nuestro método, pues en ella se pueden

integrar aspectos tecnológicos, organizativos y culturales. En ese sentido, la norma es la base de la propuesta.

Figura 11
Las normas ISO de gestión de seguridad de datos de información.

Nota. Basado en ISO/IEC 27000, ISO/IEC 27001, ISO/IEC 27002 e ISO/IEC 27005 (ISO, 2022). Tomado de Nuñez (2025).

2.1.3. Gestión de riesgos de seguridad de la información

Corresponde una parte fundamental de la seguridad de la información ya que permite que las organizaciones identifiquen, evalúen y eliminen cualquier riesgo que ponga en peligro sus activos más críticos. Según Santos Malpica (2023), "el propósito de este procedimiento es disminuir en forma considerable la probabilidad de ocurrencia de incidentes y los daños potenciales que pudieran ocasionar". La protección de los activos más críticos es una prioridad en la gestión de riesgos y asegura la continuidad de los negocios corporativos. Nuñez (2025) señala que la familia de normas ISO/IEC 27000 la define como un pilar para enmarcar políticas y controles. Lema (2025) recalca que es un proceso que se debe actualizar y mejorar continuamente, para así ajustarse a cualquier nueva amenaza o cambio que pueda surgir en la organización. Como resultado, la administración de riesgos viene a ser el eslabón entre las políticas de seguridad de la organización y lo que ésta hace en realidad.

2.1.4. Formas de abordar el análisis de riesgos

Para el proceso de gestión de riesgos se requiere de una variedad de enfoques y tecnologías capaces de evaluar de manera sistemática las vulnerabilidades y amenazas. Estas técnicas permiten anticipar fallos, minimizar pérdidas y mejorar la eficiencia en la toma de decisiones. Más allá de la ISO/IEC 27005, Lema (2025) también indica que se pueden aplicar otras técnicas complementarias, como OCTAVE, MEHARI o MAGERIT. Cada uno de estos enfoques tiene

beneficios diferentes que se ajustan mejor a las necesidades de diferentes tipos de empresas. Por ejemplo, OCTAVE es una buena elección para entornos donde la cultura corporativa es esencial, MEHARI para aquéllos que necesitan priorizar sobre la marcha y MAGERIT para organizaciones gubernamentales que necesitan mucha documentación. Estos enfoques no solo ayudan a diseñar los controles, sino que también mejoran la gestión estratégica, al permitirle dar seguimiento a cómo cambian los riesgos.

2.1.5. Marco legal LOPDP (Ecuador)

Con el fin de establecer la base jurídica para el tratamiento de datos personales, se aplicará la presente norma. Según Catota (2025)la ley obliga a las empresas a transformar sus requisitos legales en determinadas actividades técnicas y organizativas. Estas medidas incluyen el cifrado de datos sensibles, la segmentación de redes, los controles de acceso y los programas de formación. Según Morocho (2025), la LOPDP no se centra exclusivamente en la adopción de soluciones tecnológicas, sino que exige el establecimiento de procesos como la clasificación de documentos, auditorías periódicas y programas de sensibilización para los miembros del personal. Debido a que la ley se basa en conceptos como la legalidad, la lealtad, la transparencia, la proporcionalidad y la responsabilidad proactiva, es el pilar legal que debe incorporarse a cualquier sistema de gestión de la seguridad de la información basado en la norma ISO/IEC 27001. De esta manera, la incorporación de la norma técnica a la legislación local garantiza que las reglas de seguridad sean eficaces y legalmente vinculantes.

2.1.6. Los procedimientos más eficaces y la orientación práctica

La aplicación de las recomendaciones sobre mejores prácticas internacionales ayuda a aumentar la seguridad de la información financiera. La norma ISO/IEC 27002 ofrece un catálogo de controles que pueden utilizarse en diversos ámbitos, como la criptografía, la seguridad de las comunicaciones y la gestión de accesos. Según Yánez (2022), el Marco de Ciberseguridad (CSF) del NIST organiza sus acciones en cinco funciones: identificar, proteger, detectar, responder y recuperar. Estas tareas se enumeran por orden de importancia. Gracias a ello, las organizaciones pueden desarrollar planes de acción que sean sostenibles y priorizados. Verdugo (2023) indica además, que el Modelo de Madurez de Ciberseguridad (CMME) es una herramienta que ha sido ajustada a la realidad de Ecuador y que combina las normas internacionales con las particularidades del entorno ecuatoriano. La inclusión de estas normas como referencias contribuye a mejorar la propuesta, ya que permiten alinear las políticas internas con los marcos más reconocidos a nivel mundial.

2.1.7. Administración de documentos y políticas internas

La seguridad de la información además de considerar aspectos técnicos, también toma en cuenta las políticas internas y la documentación. Según Moscoso (2025), los riesgos de incumplimiento normativo aumentan debido a la ausencia de procedimientos estandarizados y la falta de definición de roles en el sector financiero ecuatoriano. Para Aguilar y Cuenca (2025), un SGSI debe desarrollar manuales, políticas, procedimientos y planes de capacitación para soportar la implementación de los controles técnicos. En este contexto, la gestión documental garantiza la aplicación uniforme de la guía y facilita los procesos de auditoría interna y externa. Además, fortalece la cultura de seguridad en la organización, comprometiéndose con la protección de la información en todos sus niveles.

2.2. Descripción de la propuesta

La propuesta es una guía para la implementación de políticas de seguridad de la información, fundamentada en la norma ISO/IEC 27001:2022 y en concordancia con la Ley Orgánica de Protección de Datos Personales (LOPDP). Busca fortalecer la protección de los activos de información de Corbantrade S.A.S., a través de un modelo estructurado desde los recursos iniciales, las etapas de administración, hasta los resultados e impacto.

2.2.1. Estructura general

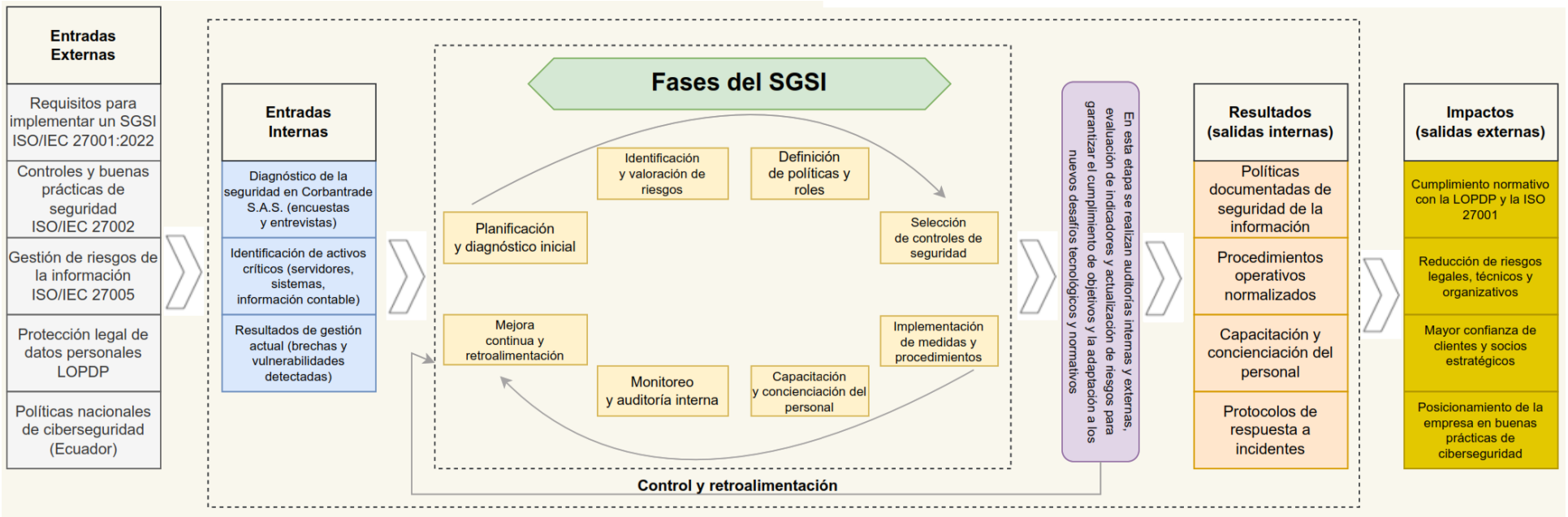
La propuesta se estructura como un modelo de entradas, procesos y salidas, el cual permite visualizar el flujo de implementación de la guía. Inicia con las fuentes externas (normas internacionales, leyes) e internas (diagnóstico de la empresa, análisis de riesgos). Estos inputs abren las etapas centrales del SGSI: la planificación, la definición de políticas y roles, la selección de controles, la capacitación del personal, los mecanismos de seguimiento y mejora continua.

Como se puede apreciar en la Figura 12, este modelo integra entradas con fases del SGSI y salidas esperadas de forma estructurada. Además, presenta resultados externos que benefician directamente a la empresa, como el aumento de la confianza del cliente.

Como resultado de estas etapas, se producen salidas internas, tales como políticas y procedimientos documentados, protocolos de respuesta y programas de capacitación. Finalmente, los beneficios externos son el cumplimiento de la LOPDP y la ISO/IEC 27001, la disminución de riesgos, la confianza del cliente y la mejora del posicionamiento de la empresa en ciberseguridad. De este modo, la guía proporciona un marco para que cada acción esté respaldada en una normativa y metodología, garantizando resultados verificables y sostenibles en el tiempo.

Figura 12

Modelo de implementación de un SGSI en Corbantrade S.A.S.



2.2.2. Explicación del aporte

La propuesta proporciona un modelo integral que guía la implementación de la seguridad de la información en Corbantrade S.A.S., a través de sus componentes interrelacionados:

- **Entradas externas**

Y esta es la ley que rige la propuesta. Dicho marco comprende la norma ISO/IEC 27001:2022, la cual especifica los requisitos para un SGSI; la ISO/IEC 27002, que proporciona un catálogo de controles y buenas prácticas; la ISO/IEC 27005, para la gestión de riesgos; la Ley Orgánica de Protección de Datos Personales (LOPDP) y las políticas ecuatorianas de ciberseguridad Estas secciones garantizan que la guía cumpla con las normativas nacionales e internacionales.

- **Entradas internas**

La guía se basa en el análisis de Corbantrade S.A.S., lo cual permitirá identificar activos críticos, vulnerabilidades y brechas de seguridad. Estos elementos son esenciales para adaptar la guía a la realidad de la empresa y garantizar que las medidas no sean estándares, sino enfocadas a la empresa.

- **Etapas del SGSI**

Estas fases constituyen el nucleo del proyecto e incluyen la planificación y el diagnóstico inicial, la identificación de riesgos, la definición de políticas y roles, la selección e implementación de controles de seguridad, la capacitación de los usuarios y los procedimientos internos de supervisión y auditoría. Todas estas acciones forman un ciclo de mejora continua que garantiza la disponibilidad de la información.

- **Resultados internos**

Son todas aquellos que permiten la continuidad del negocio, entre las cuales tenemos: las políticas de seguridad escritas, los procedimientos operativos estándar, los programas de capacitación y sensibilización de los usuarios, los protocolos de respuesta a incidentes, etc. Todo esto es esencial para fortalecer la seguridad de la información.

- **Factores externos**

En esta parte se incluye los beneficios que obtiene la empresa, entre los cuales se destacan el cumplimiento de la LOPDP y la norma ISO 27001, la reducción de riesgos legales, técnicos y operativos, el aumento de la confianza de los clientes y socios, fortaleciendo la imagen de Corbantrade S.A.S. como una empresa que se ajusta a las mejores prácticas de ciberseguridad.

2.2.3. Estrategias y/o técnicas

Para garantizar que la guía sea pertinente, práctica y duradera, se emplearon diversas tácticas y enfoques. Dentro de las cuales tenemos:

- **Revisión documental y normativa**

Se realizo una revisión de estándares internacionales como la ISO/IEC 27001:2022, ISO/IEC 27002 e ISO/IEC 27005. Así mismo, la LOPDP y las políticas nacionales de ciberseguridad del Ecuador fueron igualmente consideradas dentro de la revisión. Lo que se busca con esto es reconocer los principios, requisitos y buenas prácticas; tanto a nivel nacional como internacional, orienten a la gestión de la seguridad de la información. Con esto nos aseguramos que la guía no solo se adecúe al contexto particular de Corbantrade S.A.S., sino que también mantenga una alineación con los estándares internacionales vigentes.

- **Diagnóstico organizacional**

Además de la aplicación de encuestas y entrevistas al personal de Corbantrade S.A.S., se desarrolló un análisis para identificar las vulnerabilidades presentes en los activos críticos de la organización, entre ellos los servidores y los sistemas principales. Este diagnóstico reveló fallas en las políticas internas, falta de capacitación y riesgos en el manejo de la información. La técnica fue determinante, ya que dio una perspectiva realista de la situación actual de la empresa y así la propuesta se enfocó en resolver problemas reales y no solo teóricos.

- **Metodología de gestión de riesgos**

La propuesta se fundamentó en la norma ISO/IEC 27005, la cual proporciona una guía para la identificación, análisis y valoración de riesgos en la seguridad de la información. Esta metodología clasificó las amenazas en términos de probabilidad e impacto, lo que ayudó a elegir los mejores controles técnicos y organizativos. Con esta técnica se asegura de que la propuesta se centre en los riesgos más significativos y se aprovechen los recursos de la empresa.

- **Diseño de procesos y políticas**

Las etapas del SGSI se basaron en el ciclo PHVA (Planificar, Hacer, Verificar, Actuar). Este método asegura la mejora continua, pues en cada fase se revisan los resultados y se hacen ajustes. En esta etapa se establecieron políticas, procedimientos y responsabilidades para incorporar la seguridad de la información en la gestión de la empresa.

- **Utilización de organizadores gráficos**

Para resumir y transmitir la información de manera comprensible, se desarrollaron diagramas y esquemas visuales que representan la estructura de la propuesta, las etapas del SGSI, los resultados esperados y los impactos externos. Esta técnica hace comprensible el modelo, de manera que la alta dirección y el personal operativo comprendan cómo se aplicará la guía.

- **Validación académica y práctica**

La propuesta no es sólo un planteamiento teórico, sino que se desarrolló basándose en fuentes académicas actualizadas y se comparó con la situación actual de Corbantrade S.A.S. Esta metodología garantiza que el resultado sea un producto con rigor científico y práctico, haciéndolo útil para fines institucionales y de cumplimiento normativo.

Finalmente, todo lo planteado en la propuesta se materializó en una Guía para la implementación de políticas de seguridad de la información en Corbantrade S.A.S., este documento se estructura en capítulos que abarcan desde los fundamentos conceptuales hasta los recursos prácticos aplicables. La guía fue creada como una herramienta de referencia interna, pero también puede ser aplicada en otras organizaciones que enfrenten necesidades semejantes. Para efectos de precisión y utilidad, la versión completa se incluye en el Anexo 11, donde se recopilan todos los apartados, recursos y formatos desarrollados en este proyecto.

2.3. Validación de la propuesta

Para la validación de la propuesta se usó el método de criterios de especialistas. Esta metodología permite determinar la adecuación, factibilidad y usabilidad del producto diseñado a través de la opinión de especialistas en seguridad de la información. Esto se hizo de acuerdo a las siguientes etapas:

- **Selección de especialistas**

Se seleccionaron especialistas y académicos con experiencia en seguridad de la información, gestión de riesgos, aplicación de la norma ISO/IEC 27001 y cumplimiento de la LOPDP. La elección se fundamentó en criterios como la formación académica, la trayectoria profesional y la participación en proyectos de naturaleza semejante.

- **Instrumento de validación**

Fue elaborada una matriz de evaluación con indicadores específicos, estructurados en tres dimensiones:

- ✓ La primera corresponde a la adecuación, donde se examina si la propuesta satisface las necesidades de la organización y los requerimientos actuales en materia de seguridad de la información, además de confirmar su alineación con las normas y regulaciones técnicas nacionales e internacionales.
- ✓ La segunda dimensión se centra en la factibilidad, la cual determina si la propuesta puede implementarse con los recursos financieros, humanos y tecnológicos disponibles, valorando la viabilidad de los objetivos planteados y la suficiencia de la infraestructura y del personal.
- ✓ Finalmente, la tercera dimensión considera la contribución académica y práctica, enfocada en evaluar el aporte de la propuesta al campo de la seguridad de la información y su capacidad para ofrecer soluciones aplicables en el ámbito profesional. Esta dimensión incluye la valoración de su eficacia teórica y práctica, con el propósito de optimizar procesos, fortalecer la seguridad de la información y respaldar la toma de decisiones en la organización.

- **Validación de resultados**

La propuesta fue valorada de manera positiva por la mayoría de los especialistas, quienes destacaron que responde adecuadamente a las necesidades actuales de la empresa en materia de protección de datos e información sensible. También remarcaron su factibilidad, al sustentarse en metodologías reconocidas a nivel internacional y adaptarse de forma pertinente al contexto ecuatoriano. Finalmente, señalaron su aporte académico al vincular la LOPDP con la norma ISO/IEC 27001 y compararla con las tendencias globales en protección de datos.

- **Análisis de resultados de los especialistas**

El Mgs. Galo David Cárdenas C., evaluó con 32 puntos, lo que equivale al 91%. En su evaluación, resaltó la aplicabilidad, la fundamentación tecnológica y la pertinencia del trabajo. En sus observaciones, él observó que la guía es un recurso útil que se adapta bien a las necesidades de Corbantrade S.A.S., lo cual la hace práctica. Asimismo, propuso optimizar los contenidos pedagógicos utilizando ejemplos simples y materiales suplementarios, como guías rápidas o manuales, de modo que el personal no técnico tenga una mejor comprensión de las directrices. En el Anexo 10 se encuentran los resultados totales de su evaluación.

La Mgs. María Fernanda Palma A. evaluó con 31 puntos, lo que equivale al 89%, resaltó la claridad estructural y la solidez técnica del mismo. En su opinión, la propuesta satisface las necesidades de Corbantrade S.A.S. y se encuentra conforme con las directrices normativas

actuales. Sugirió, con la intención de robustecer la sensibilización y el aprendizaje en todos los niveles de la organización, mejorar la base pedagógica mediante la inclusión de actividades prácticas de capacitación e infografías explicativas. Su informe de validación tiene más detalles en el Anexo 12.

En conclusión, ambos especialistas coincidieron en que la propuesta es viable, ya que satisface las necesidades de seguridad de la información de Corbantrade S.A.S. y se ajusta a todas las leyes pertinentes. Entre las principales recomendaciones están el añadir más recursos didácticos y reforzar el componente pedagógico. Estos se tuvieron en cuenta para mejorar la versión final de la guía. De este modo, se confirma que el proyecto es una herramienta útil, aplicable y sostenible para gestionar la seguridad de la información dentro de la empresa.

2.4. Matriz de articulación de la propuesta

La siguiente matriz ofrece un resumen conciso de la articulación del producto que se generó utilizando los fundamentos teóricos, metodológicos, estratégico-técnicos y tecnológicos que se utilizaron. Según la información presentada en la Tabla 1, la propuesta incorpora los ejes principales junto con sus respectivos fundamentos teóricos, metodológicos y técnicos. Esto garantiza la coherencia entre el marco normativo, la metodología utilizada y los resultados previstos.

Tabla 1

Matriz de articulación de la propuesta

EJES O PARTES PRINCIPALES	SUSTENTO TEÓRICO	SUSTENTO METODOLÓGICO	ESTRATEGIAS / TÉCNICAS	DESCRIPCIÓN DE RESULTADOS	INSTRUMENTOS APLICADOS
Seguridad de la información	Principios de confidencialidad, integridad y disponibilidad sustentados en la norma ISO/IEC 27001:2022 y en los aportes de Aguilar y Cuenca (2025).	Investigación documental y revisión bibliográfica.	Análisis de normativa ISO/IEC y alineación con la LOPDP.	Identificación de los fundamentos que sustentan la propuesta.	Fichas de análisis documental.
ISO/IEC 27001:2022	Requisitos para la implementación de un SGSI (Nuñez 2025) y las normas ISO (Ávila 2024).	Ciclo PHVA (Planificar, Hacer, Verificar, Actuar).	Adaptación de la norma al contexto de Corbantrade S.A.S.	Diseño de lineamientos basados en la norma internacional.	Guías normativas ISO.
Gestión de riesgos	Identificación, análisis y tratamiento de riesgos (Lema 2025).	Enfoque cualitativo–cuantitativo mediante matriz de riesgos.	Aplicación de metodologías de análisis (ISO 27005, OCTAVE, MEHARI, MAGERIT).	Definición de controles y priorización de medidas de seguridad.	Matriz de riesgos y entrevistas internas.
Marco legal (LOPDP)	Derechos de privacidad, intimidad y autodeterminación informativa (Ley Orgánica de Protección de Datos Personales 2021).	Revisión normativa y análisis comparativo.	Análisis de cumplimiento legal y alineación con ISO/IEC 27001.	Garantía de conformidad legal en la propuesta.	Guía oficial de la LOPDP y comparación con GDPR.
Validación de la propuesta	Pertinencia, viabilidad y aporte académico–práctico (Verdugo 2023).	Evaluación por criterios de especialistas.	Matriz de validación por especialistas.	Confirmación de la relevancia y aplicabilidad de la guía.	Instrumento de validación con escalas de valoración.

CONCLUSIONES

Este proyecto demostró que la implementación de un Sistema de Gestión de Seguridad de la Información en Corbantrade S.A.S., basado en la norma ISO/IEC 27001:2022 y alineado con la LOPDP, es un factor esencial para garantizar la protección de la información crítica de la organización. Esto quedó demostrado a lo largo del proyecto. Adoptar este enfoque no solo satisface la necesidad de cumplir con los requisitos actualmente vigentes, sino que también ayuda a cultivar una cultura dentro de la empresa centrada en la prevención de riesgos y la mejora continua de los procedimientos de seguridad de la información.

Sobre la base de la identificación del marco teórico y jurídico que sustenta la propuesta, se hizo hincapié en la importancia de los principios de confidencialidad, integridad y disponibilidad como pilares de un SGSI. El desarrollo de políticas, controles y procesos que garanticen una gestión eficaz de la información y prevengan incidentes que puedan afectar a la estabilidad operativa o la reputación de la empresa se basa en estos principios reconocidos internacionalmente, que sirven de base para el desarrollo de estas políticas y procedimientos.

Los analices realizados en Corbantrade S.A.S. se evidenciaron deficiencias en la parte legal, tecnológico y organizativo. Esto permitió afianzar la necesidad de implementar metodologías estructuradas como: MAGERIT, ISO/IEC 27005 y OCTAVE, las mismas que permiten clasificar las medidas de control en función del tipo de activos y riesgos identificados. De esta forma se considera que estos enfoques contribuyen a reducir los riesgos y garantizar la continuidad operativa de la empresa, esto se da porque, las medidas implementadas no son seleccionadas de forma aleatoria, sino en el marco de una estrategia organizada y evaluable.

La guía articula los estándares internacionales de seguridad con el marco legal ecuatoriano establecido en la LOPDP. Esta integración asegura el cumplimiento normativo y, al mismo tiempo, otorga a la organización una ventaja competitiva dentro de su sector.

Los resultados obtenidos permiten evidenciar dos áreas afectadas de manera positiva, en el ámbito académico, constituye un marco metodológico susceptible de ser replicado en otras firmas de auditoría y contabilidad, lo cual contribuye a la mejora en la adopción de buenas prácticas de seguridad de la información y al fortalecimiento del conocimiento. Así mismo, en la parte práctica, brinda a Corbantrade S.A.S. una herramienta adaptada a su realidad operativa, la cual es reconocida por su aplicabilidad, pertinencia y sostenibilidad en el tiempo.

RECOMENDACIONES

Desde mi punto de vista la organización requiere implementar un proceso continuo de actualización y capacitación en seguridad de la información y protección de datos. La adopción de esto resulta indispensable para que las políticas y procedimientos puedan ajustarse oportunamente frente a la aparición de nuevos riesgos tecnológicos. La ejecución de este proceso no debe limitarse a una formación general, sino que debe contemplarse de acuerdo con el rol de cada usuario, de manera que cada uno cuente con las herramientas necesarias para aplicar las medidas de seguridad en su espacio de trabajo.

Para poder asegurar el correcto funcionamiento del Sistema de Gestión de Seguridad de la Información, se debe considera reforzar los mecanismos de control, realizando revisiones continuas y una auditoría interna. Estos deben contar con indicadores precisos y verificables que permitan medir el grado de cumplimiento de los objetivos. A si mismo, se debe complementar estas prácticas con auditorías externas periódicas, esto permitirá confirmar la eficacia de los controles aplicados, permitiendo una visión diferente sobre el nivel de madurez alcanzado en la gestión de la seguridad.

Se debe tener en cuenta el poder alinear el SGSI con marcos internacionales adicionales, como el Cybersecurity Framework (CSF) del Instituto Nacional de Estándares y Tecnología (NIST) o el modelo de madurez en capacidades de ciberseguridad (C2M2). La incorporación de estos marcos permitiría ampliar la visión de la empresa en torno a la madurez en ciberseguridad, de esta manera poder establecer comparaciones con estándares regionales e internacionales, facilitando así la identificación de buenas prácticas replicables en Corbantrade S.A.S.

Así mismo, se debe divulgar los resultados del proyecto en espacios académicos y profesionales, tales como: seminarios, congresos o publicaciones especializadas; esto permitirá no solo fortalecer la cultura de seguridad de la información en Corbantrade S.A.S., sino que también serviría para reforzarla en otras pymes del sector contable y de auditoría. En consecuencia, se tendrá un entorno empresarial más consciente de los desafíos relacionados con la protección de datos en la era digital actual y una mayor capacidad para enfrentarlos de manera eficaz.

BIBLIOGRAFÍA

Aguilar, C., y Cuenca, J. (2025). Diseño de un sistema de gestión de seguridad de la información (SGSI) basado en el estándar ISO/IEC 27001 para la empresa EJEPROY CIA. LTDA. *MQRInvestigar* , *9*(1), e361. https://doi.org/10.56048/MQR20225.9.1.2025.e361

Ávila, A. (2024, October). *MODELO DE SGSI EN EL DEPARTAMENTO DE TI DEL GADMCN, APLICANDO CONTROLES ISO/IEC 27001:2013 E ISO/IEC 27002:2022*. https://ciencialatina.org/index.php/cienciala/article/view/14503/20715

Catota, A. (2025). *PROPUESTA DE UNA MEJORA DE LA SEGURIDAD DE LA INFORMACIÓN EN UN NEGOCIO FIDUCIARIO DANDO CUMPLIMIENTO A LA LEY DE PROTECCIÓN DE DATOS PERSONALES EN EL ECUADOR USANDO UNA PRUEBA DE CONCEPTO Y PROPONIENDO UNA CONTRAMEDIDA*.

Lema, oscar. (2025). *Propuesta de un sistema de seguridad de la información para una Empresa de Telecomunicaciones bajo la Norma ISO/IEC 27005*. http://repositorio.uisrael.edu.ec/bitstream/47000/4305/1/UISRAEL-EC-MASTER-SEG-INF-PRO-378.242-2025-004.pdf

Ley Orgánica de Protección de Datos Personales. (2021). *Ley Orgánica de Protección de Datos Personales*.

Morocho, C. (2025). *Buenas prácticas para el cumplimiento de la Ley de Protección de Datos Personales en el Sistema Nacional de Rendición de Cuentas bajo las Normas ISO/IEC 27001*. http://repositorio.uisrael.edu.ec/bitstream/47000/4309/1/UISRAEL-EC-MASTER-SEG-INF-PRO-378.242-2025-008.pdf

Moscoso, J. (2025). *"EVALUACIÓN JURÍDICA DE RIESGOS Y VULNERABILIDADES EN LA PROTECCIÓN DE DATOS EN INSTITUCIONES FINANCIERAS DEL ECUADOR BAJO LA LEY ORGÁNICA DE PROTECCIÓN DATOS PERSONALES."* https://dspace.ucacue.edu.ec/server/api/core/bitstreams/de4b613c-519b-4f9c-9852-8d18ac21e733/content

Nuñez, D. (2025). *Modelo para la Gestión de Seguridad de la Información en Cooperativas de Ahorro y Crédito del Segmento 1 Basada en ISO/IEC 27001:2022*. http://repositorio.uisrael.edu.ec/bitstream/47000/4312/1/UISRAEL-EC-MASTER-SEG-INF-PRO-378.242-2025-011.pdf

Politica de Ciberseguridad (2021). https://www.telecomunicaciones.gob.ec/wp-content/uploads/2021/06/Acuerdo-No.-006-2021-Politica-de-Ciberseguridad.pdf

Política Nacional de Ciberseguridad. (2021). *Política Nacional de Ciberseguridad*.

Romero, I. (2024). *CUMPLIMIENTO DE LA NORMATIVA DE SEGURIDAD DE LA INFORMACIÓN, PARA LA COAC ACHIK INTI DEL CANTÓN CAÑAR, SEGMENTO 4 Y SU PROGRESIÓN AL SEGMENTO 3, BAJO LA REGULACIÓN DE LA SEPS.*

Santos Malpica, I. (2023). *CTFs como medio de aprendizaje en la ciberseguridad*. Universidad Nacional de Educación a Distancia (España). Escuela Técnica Superior de Ingeniería Informática. https://e-spacio.uned.es/entities/publication/4a959d7c-2b9b-4a7d-acbc-e17d3f06e795

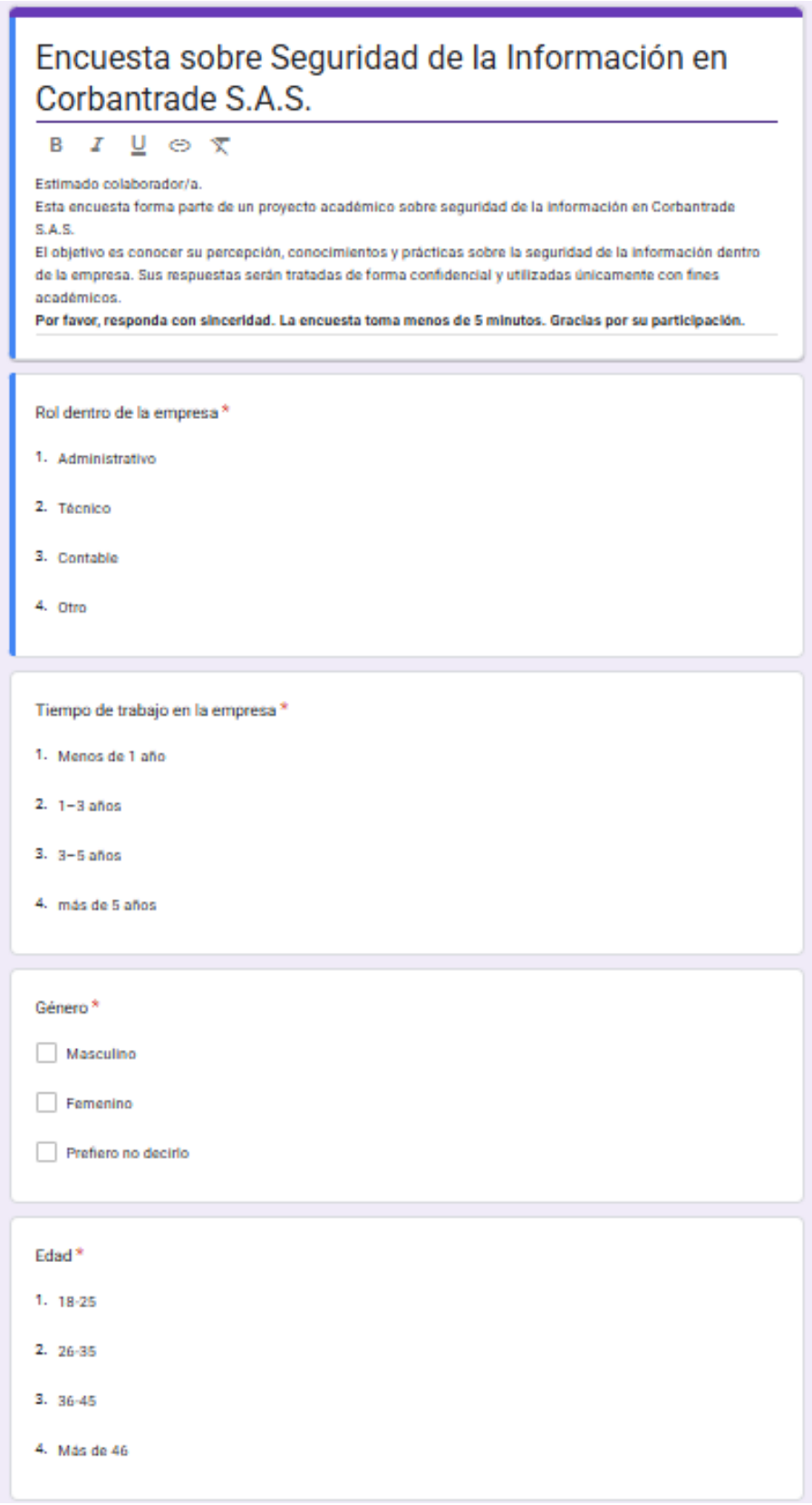
Verdugo, G. (2023). *"PROPUESTA DE UN MODELO DE MADUREZ DE CIBERSEGURIDAD PARA ECUADOR."* https://dspace.ucacue.edu.ec/server/api/core/bitstreams/bb62d854-ad21-4ef0-ac9e-2731ba7ea16c/content

Yagual, G. (2024). *DESARROLLO DE UNA GUÍA DE IMPLEMENTACIÓN DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (SGSI) PARA EL DEPARTAMENTO DE SISTEMAS DEL GAD MUNICIPAL DE LA LIBERTAD*.

Yánez, J. (2022). *APLICACIÓN DEL "NIST CYBERSECURITY FRAMEWORK" EN EL INSTITUTO SUPERIOR TECNOLÓGICO "SUCRE."* https://repositorio.puce.edu.ec/server/api/core/bitstreams/1db0ae0e-c10e-4a07-8e19-4c721d726eec/content

ANEXOS

ANEXO 1



Encuesta sobre Seguridad de la Información en Corbantrade S.A.S.

Estimado colaborador/a.
Esta encuesta forma parte de un proyecto académico sobre seguridad de la información en Corbantrade S.A.S.
El objetivo es conocer su percepción, conocimientos y prácticas sobre la seguridad de la información dentro de la empresa. Sus respuestas serán tratadas de forma confidencial y utilizadas únicamente con fines académicos.
Por favor, responda con sinceridad. La encuesta toma menos de 5 minutos. Gracias por su participación.

Rol dentro de la empresa *

1. Administrativo
2. Técnico
3. Contable
4. Otro

Tiempo de trabajo en la empresa *

1. Menos de 1 año
2. 1–3 años
3. 3–5 años
4. más de 5 años

Género *

- [ ] Masculino
- [ ] Femenino
- [ ] Prefiero no decirlo

Edad *

1. 18-25
2. 26-35
3. 36-45
4. Más de 46

FORMATO DE ENCUESTA

ANEXO 2

INSTRUCCIONES PARA LAS PREGUNTAS

A continuación, encontrará una serie de afirmaciones. Marque el nivel de acuerdo o desacuerdo según su experiencia. Se utiliza una escala de 1 a 5 donde:

1 = Totalmente en desacuerdo, 2 = En desacuerdo, 3 = Ni de acuerdo ni en desacuerdo, 4 = De acuerdo, 5 = Totalmente de acuerdo

1. Conozco los principios generales de la norma ISO/IEC 27001. *

1 2 3 4 5

2. Tengo noción de los derechos que establece la Ley Orgánica de Protección de Datos Personales (LOPDP). *

1 2 3 4 5

3. En la empresa existen políticas claras sobre el manejo de información confidencial. *

1 2 3 4 5

4. Se aplican buenas prácticas para el manejo de contraseñas y accesos. *

1 2 3 4 5

5. He recibido capacitación sobre seguridad de la información o protección de datos. *

1 2 3 4 5

6. Considero que los sistemas de respaldo de información están correctamente implementados. *

1 2 3 4 5

7. El acceso a los sistemas de la empresa está adecuadamente controlado. *

1 2 3 4 5

8. Uso buenas prácticas al manejar información sensible (clientes, finanzas, etc.). *

FORMATO DE ENCUESTA PREGUNTAS

ANEXO 3

Entrevista Administrativa – Seguridad de la Información en Corbantrade S.A.S.

Estimada Msc. Gallo.

Este formulario es parte de una entrevista administrativa para el proyecto de titulación "Guía para la implementación de políticas de seguridad de la información según la norma ISO/IEC 27001, alineada a la Ley Orgánica de Protección de Datos Personales en Corbantrade S.A.S.".

Le solicitamos que responda con base en su conocimiento sobre el funcionamiento interno de la empresa. Las respuestas serán confidenciales y utilizadas únicamente con fines académicos.

Gracias por su colaboración y tiempo.

1. ¿La empresa cuenta con políticas claras para el manejo de datos de clientes? *

Texto de respuesta larga

2. ¿Ha recibido alguna capacitación sobre protección de datos personales o seguridad informática? *

Texto de respuesta larga

3. ¿Cómo se protegen los documentos o archivos sensibles dentro del área administrativa? *

Texto de respuesta larga

4. ¿Existen procedimientos en caso de incidentes de seguridad digital? *

Texto de respuesta larga

5. ¿Qué tan prioritario cree usted que es implementar políticas de seguridad de la información? *

Texto de respuesta larga

6. ¿Considera útil una guía estructurada basada en normas como la ISO/IEC 27001 y la LOPDP? *

FORMATO DE ENTREVISTA ADMINISTRACIÓN

ANEXO 4

Entrevista Técnica – Seguridad de la Información en Corbantrade S.A.S.

Estimado Ing. Torres.

Este formulario es parte de una entrevista técnica para el proyecto de titulación "Guía para la implementación de políticas de seguridad de la información según la norma ISO/IEC 27001, alineada a la Ley Orgánica de Protección de Datos Personales en Corbantrade S.A.S.".

Le pedimos que responda con base en su experiencia en el área de sistemas. Sus respuestas serán confidenciales y se usarán únicamente con fines académicos.

Agradezco de antemano su tiempo y claridad en las respuestas.

1. ¿Qué controles de seguridad están actualmente implementados en la red y los servidores? *

Texto de respuesta larga

2. ¿Existen políticas formales para la gestión de accesos y contraseñas? *

Texto de respuesta larga

3. ¿Cómo se realiza el respaldo de la información crítica? *

Texto de respuesta larga

4. ¿Se ha presentado algún incidente de seguridad en los últimos años? ¿Cómo fue gestionado? *

Texto de respuesta larga

5. ¿Qué desafíos enfrenta el área de TI en términos de seguridad informática? *

Texto de respuesta larga

6. ¿Considera necesaria una guía para implementar buenas prácticas de seguridad en la empresa? *

FORMATO DE ENTREVISTA SISTEMAS

ANEXO 5

CHARLA AL PERSONAL DE CORBANTRADE S.A.S.

ANEXO 6

OBJETIVOS DE LA GUÍA

ANEXO 7

MODELO DE IMPLEMENTACIÓN

ANEXO 8

RIESGOS DE SEGURIDAD DETECTADOS

ANEXO 9

UNIVERSIDAD TECNOLÓGICA ISRAEL

ESCUELA DE POSGRADOS "ESPOG"

MAESTRÍA EN SEGURIDAD INFORMÁTICA

VINCULACIÓN CON LA SOCIEDAD

Tema:
"GUÍA PARA LA IMPLEMENTACIÓN DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN SEGÚN LA NORMA ISO/IEC 27001 PARA LA INFRAESTRUCTURA Y EQUIPAMIENTO DE LA EMPRESA CORBANTRADE S.A.S."
Fecha:
Quito, 01 de septiembre de 2025
Autor:
Juan Carlos Cumbicus Bravo
Enlace:
https://drive.google.com/drive/folders/1RLoMCuGuxmWEuZzDHMv1FFBBGs-TAsMz?usp=sharing

Quito – Ecuador

2025

EVIDENCIA DE LA CHARLA

ANEXO 10

Universidad Israel
ESPOG | Escuela de Posgrados

UNIVERSIDAD TECNOLÓGICA ISRAEL

ESCUELA DE POSGRADOS "ESPOG"

MAESTRÍA EN SEGURIDAD INFORMÁTICA

INSTRUMENTO PARA VALIDACIÓN DE LA PROPUESTA

Estimado colega:

Se solicita su valiosa cooperación para evaluar la calidad del siguiente contenido digital **"GUÍA PARA LA IMPLEMENTACIÓN DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN SEGÚN LA NORMA ISO/IEC 27001 PARA LA INFRAESTRUCTURA Y EQUIPAMIENTO DE LA EMPRESA CORBANTRADE S.A.S."**. Sus criterios son de suma importancia para la realización de este trabajo, por lo que se le pide que brinde su cooperación contestando las preguntas que se realizan a continuación.

Datos informativos

Validado por: Galo David Cárdenas Calderón
Título obtenido: Magíster en Tecnologías de la Información, mención en Seguridad de Redes y Comunicaciones.
C.I.: 1716129547
E-mail: gcardenas@tecentel.com
Institución de Trabajo: Tecentel S.A.
Cargo: Presidente
Años de experiencia en el área: 15

Universidad Israel
ESPOG | Escuela de Posgrados

Instructivo:

- Responda cada criterio con la máxima sinceridad del caso.
- Revisar, observar y analizar la propuesta de la plataforma virtual, blog o sitio web.
- Coloque una X en cada indicador, tomando en cuenta que Muy adecuado equivale a 5, Bastante Adecuado equivale a 4, Adecuado equivale a 3, Poco Adecuado equivale a 2 e Inadecuado equivale a 1.

Tema: "GUÍA PARA LA IMPLEMENTACIÓN DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN SEGÚN LA NORMA ISO/IEC 27001 PARA LA INFRAESTRUCTURA Y EQUIPAMIENTO DE LA EMPRESA CORBANTRADE S.A.S."

Indicadores	Muy adecuado	Bastante Adecuado	Adecuado	Poco adecuado	Inadecuado
Pertinencia	X				
Aplicabilidad	X				
Factibilidad		X			
Novedad		X			
Fundamentación pedagógica		X			
Fundamentación tecnológica	X				
Indicaciones para su uso	X				
TOTAL	32				

Observaciones: Considero que esta guía tiene un enfoque muy útil y está bien adaptada al contexto de Corbantrade S.A.S., lo que la hace muy pertinente y aplicable. La fundamentación técnica es sólida, de modo que la implementación no debería presentar mayores dificultades.
Recomendaciones: Sugiero reforzar los contenidos pedagógicos con ejemplos más sencillos y recursos de apoyo como manuales o guías rápidas, de manera que el personal no técnico logre asimilar con mayor facilidad las directrices establecidas.

Lugar, fecha de validación: Quito, 29 de agosto de 2025.

GALO DAVID CÁRDENAS CALDERÓN

Firma del especialista
Mgs. Galo David Cárdenas C.

EVALUACIÓN ESPECIALISTA 1

ANEXO 11

Universidad Israel
ESPOG | Escuela de Posgrados

UNIVERSIDAD TECNOLÓGICA ISRAEL

ESCUELA DE POSGRADOS "ESPOG"

MAESTRÍA EN SEGURIDAD INFORMÁTICA

INSTRUMENTO PARA VALIDACIÓN DE LA PROPUESTA

Estimado colega:

Se solicita su valiosa cooperación para evaluar la calidad del siguiente contenido digital **"GUÍA PARA LA IMPLEMENTACIÓN DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN SEGÚN LA NORMA ISO/IEC 27001 PARA LA INFRAESTRUCTURA Y EQUIPAMIENTO DE LA EMPRESA CORBANTRADE S.A.S."**. Sus criterios son de suma importancia para la realización de este trabajo, por lo que se le pide que brinde su cooperación contestando las preguntas que se realizan a continuación.

Datos informativos

Validado por: María Fernanda Palma Agama
Título obtenido: Magíster en Tecnologías de la Información, mención en Seguridad y Redes
C.I.: 0502477649
E-mail: fpalma@tecentel.com
Institución de Trabajo: Tecentel S.A.
Cargo: Representante legal
Años de experiencia en el área: 15

Universidad Israel
ESPOG | Escuela de Posgrados

Instructivo:

- Responda cada criterio con la máxima sinceridad del caso.
- Revisar, observar y analizar la propuesta de la plataforma virtual, blog o sitio web.
- Coloque una X en cada indicador, tomando en cuenta que Muy adecuado equivale a 5, Bastante Adecuado equivale a 4, Adecuado equivale a 3, Poco Adecuado equivale a 2 e Inadecuado equivale a 1.

Tema: "GUÍA PARA LA IMPLEMENTACIÓN DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN SEGÚN LA NORMA ISO/IEC 27001 PARA LA INFRAESTRUCTURA Y EQUIPAMIENTO DE LA EMPRESA CORBANTRADE S.A.S."

Indicadores	Muy adecuado	Bastante Adecuado	Adecuado	Poco adecuado	Inadecuado
Pertinencia	X				
Aplicabilidad		X			
Factibilidad		X			
Novedad		X			
Fundamentación pedagógica		X			
Fundamentación tecnológica	X				
Indicaciones para su uso	X				
TOTAL	31				

Observaciones: En mi criterio, la propuesta se ajusta bien a las necesidades de Corbantrade S.A.S. y cumple con los lineamientos normativos. Destaco la solidez técnica y la claridad en su estructura.
Recomendaciones: Recomiendo enriquecer la fundamentación pedagógica mediante la inclusión de infografías explicativas y actividades prácticas de capacitación, con el fin de fortalecer el proceso de sensibilización y aprendizaje en todos los niveles de la organización.

Lugar, fecha de validación: Quito, 29 de agosto de 2025.

MARIA FERNANDA PALMA AGAMA

Firma del especialista
Mgs. María Fernanda Palma A.

EVALUACIÓN ESPECIALISTA 2

ANEXO 12

UNIVERSIDAD TECNOLÓGICA ISRAEL

Título:

GUÍA PARA LA IMPLEMENTACIÓN DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN SEGÚN LA NORMA ISO/IEC 27001 PARA LA INFRAESTRUCTURA Y EQUIPAMIENTO DE LA EMPRESA CORBANTRADE S.A.S.

Autor:

Ing. Juan Carlos Cumbicus Bravo

Año de Publicación:

Quito – Ecuador

2025

PÁGINA LEGAL

El objetivo de esta guía es ayudar a cumplir los requisitos del Máster en Seguridad de la Información que ofrece la Universidad Tecnológica de Israel. Esta guía se titula “Guía para la implementación de políticas de seguridad de la información según la norma ISO/IEC 27001 para la infraestructura y los equipos de la empresa Corbantrade S.A.S.”.

AGRADECIMIENTO

Quiero expresar mi gratitud a Dios y a mi familia por proporcionarme la perseverancia que necesitaba para completar este año académico. Su comprensión, paciencia y apoyo han sido inestimables.

Me gustaría expresar mi gratitud a los profesores del Máster en Seguridad Informática de la Universidad Tecnológica de Israel por compartir sus conocimientos y ayudarme a escribir este trabajo.

En particular, me gustaría expresar mi gratitud a Corbantrade S.A.S. por proporcionarme información valiosa y permitirme utilizar herramientas de investigación que fueron cruciales para el desarrollo de esta guía.

Juan Carlos Cumbicus Bravo

Tabla de contenido

INTRODUCCIÓN

Contextualización del tema

Como señala Romero (2024), uno de los recursos más importantes para las empresas en la economía digital moderna es la información. Una empresa que ofrece servicios de consultoría contable y financiera es Corbantrade S.A.S. Gestiona datos extremadamente sensibles, incluidos registros contables, documentos internos e información de clientes. El acceso no autorizado, las fugas de información y el incumplimiento normativo son más probables debido a la ausencia de protocolos de seguridad estandarizados. Para proteger los activos de información y mantener las operaciones comerciales en este entorno, es imprescindible aplicar la Ley Orgánica de Protección de Datos Personales (LOPDP) y la norma ISO/IEC 27001:2022.

Objetivo de la guía

En línea con lo propuesto por Yagual (2024), esta guía busca ofrecer a Corbantrade S.A.S. un conjunto de pautas claras y organizadas que le posibiliten establecer políticas de seguridad de la información en conformidad con la LOPDP y la norma ISO/IEC 27001:2022. El propósito de la guía es ser un instrumento práctico que apoye el cumplimiento de la ley, la gestión de los riesgos y el fortalecimiento de la cultura organizacional en torno a la protección de datos.

Público objetivo

La guía está dirigida principalmente al personal administrativo, contable, técnico y directivo de Corbantrade S.A.S., quienes desempeñan un papel fundamental en la gestión y protección de la información de la organización. Estos grupos son responsables de garantizar que los procesos internos relacionados con datos sensibles se lleven a cabo de manera segura y conforme a la normativa vigente. La inclusión de todos los niveles jerárquicos asegura que la seguridad de la información no se limite únicamente al área de sistemas, sino que se convierta en un compromiso transversal dentro de la organización.

De igual forma, esta guía resulta aplicable a pequeñas y medianas empresas (PYMEs) del sector contable y financiero que enfrentan desafíos similares en el cumplimiento normativo y la implementación de políticas de seguridad de la información. La experiencia de Corbantrade S.A.S. sirve como caso práctico que puede ser replicado en otras organizaciones que, al igual que esta, manejan datos personales, financieros y contables de alta criticidad. Por lo tanto, el

documento se constituye en un recurso útil no solo para la empresa objeto de estudio, sino también como referencia metodológica para entidades que buscan alinear su gestión de la información con estándares internacionales como la ISO/IEC 27001 y la LOPDP.

Metodología utilizada

La elaboración de esta guía se fundamentó en un enfoque metodológico mixto, combinando técnicas cualitativas y cuantitativas. En la fase cuantitativa se aplicaron encuestas estructuradas al personal administrativo y operativo de Corbantrade S.A.S., con el fin de identificar el nivel de conocimiento y percepción en torno a la seguridad de la información. En el componente cualitativo se llevaron a cabo entrevistas semiestructuradas con miembros clave de la organización, lo que permitió profundizar en aspectos técnicos, organizativos y legales vinculados a la protección de datos.

Paralelamente, se realizó una revisión exhaustiva de literatura académica, documentos normativos y estándares internacionales, destacando la ISO/IEC 27001:2022, la ISO/IEC 27002 y la ISO/IEC 27005, así como la Ley Orgánica de Protección de Datos Personales (LOPDP) y la Política Nacional de Ciberseguridad. Este contraste entre el marco teórico y la práctica organizacional proporcionó una base sólida para diseñar la guía, asegurando que las recomendaciones estén respaldadas tanto por evidencia académica como por la realidad operativa de la empresa.

Cómo utilizar la guía

La guía está estructurada en secciones temáticas que facilitan un proceso ordenado y progresivo para implementar políticas de seguridad de la información. Cada capítulo combina fundamentos teóricos, recomendaciones prácticas y herramientas de apoyo que guían al lector desde el diagnóstico inicial hasta la validación de resultados.

Se recomienda que los usuarios sigan el orden propuesto, ya que cada sección está diseñada para construir sobre la anterior, permitiendo que el proceso sea lógico y acumulativo. Sin embargo, la flexibilidad del documento permite adaptar las orientaciones a las circunstancias particulares de la empresa, priorizando los controles o fases que resulten más urgentes según el contexto.

Capítulo I: Fundamentos teóricos y conceptuales

1.1. Conceptos clave

Tal como afirman Aguilar y Cuenca (2025), la seguridad de la información se sostiene en tres principios esenciales:

1.1.1. Seguridad de la información

Se basa en tres principios esenciales.

- **Confidencialidad**

Asegúrese de que solo puedan ver la información aquellas personas autorizadas para ello.

- **Integridad**

Haga que los datos sean accesibles cuando sea necesario.

- **Disponibilidad**

Es fundamental garantizar que los usuarios autorizados tengan acceso a la información cuando la necesiten.

1.1.2. Norma ISO/IEC 27001:2022

Como señala Nuñez (2025), esta norma es un estándar internacional que indica cómo establecer un Sistema de Gestión de Seguridad de la Información (SGSI). Proporciona controles y prácticas óptimas que te ayudan a cumplir las normas y reducir tus riesgos.

Asimismo, la ISO/IEC 27001 se complementa con otras normas de la familia, como la ISO/IEC 27002, que establece un catálogo de controles y buenas prácticas; y la ISO/IEC 27005, orientada a la gestión de riesgos. Tal como indica Lema (2025), esta integración permite a las organizaciones identificar vulnerabilidades críticas y priorizar acciones, garantizando la continuidad del negocio y el cumplimiento normativo.

1.1.3. Gestión de riesgos

Es un proceso clave dentro de la seguridad de la información, ya que permite identificar y tratar amenazas que afectan a los activos críticos. De acuerdo con Santos Malpica (2023), el propósito de este procedimiento es reducir la probabilidad de incidentes y sus daños asociados. Asimismo, Lema (2025) destaca que la gestión de riesgos debe ser un proceso dinámico, sujeto a actualización continua, mientras que Nuñez (2025) lo considera un eje fundamental dentro de

la familia de normas ISO/IEC 27000, al servir de puente entre las políticas y los controles aplicados en la práctica.

1.1.4. Ley Orgánica de Protección de Datos Personales (LOPDP)

Según Catota (2025), la LOPDP obliga a las organizaciones a traducir sus obligaciones legales en medidas técnicas y organizativas concretas, como cifrado, controles de acceso y segmentación de redes. En la misma línea, Morocho (2025) subraya que la ley no se limita a la aplicación de medidas tecnológicas, sino que también exige procesos de sensibilización y auditorías periódicas.

1.2. Importancia del tema

En un mundo empresarial que se vuelve cada vez más digital, la información es uno de los activos más valiosos. Para una compañía de servicios contables y financieros como Corbantrade S.A.S., es crucial proteger esa información por varias razones:

- **Cumplimiento legal**

De acuerdo con Catota (2025), el cumplimiento de la LOPDP implica traducir las obligaciones legales en medidas técnicas concretas como cifrado y segmentación de redes, lo cual evita sanciones legales.

- **Confianza del cliente**

Tal como señalan Aguilar y Cuenca (2025), la certificación bajo ISO/IEC 27001 no solo refuerza la seguridad de la información, sino que también genera confianza en clientes y socios estratégicos.

- **Prevención de incidentes**

En línea con lo expuesto por Lema (2025), contar con políticas claras y controles de seguridad permite reducir de manera considerable la ocurrencia de incidentes de ciberseguridad.

- **Continuidad del negocio**

Romero (2024)indica que la seguridad de la información es un factor estratégico para garantizar la continuidad de las operaciones en un entorno cada vez más digitalizado.

- **Competitividad**

De acuerdo con Verdugo (2023), las empresas que avanzan en madurez de ciberseguridad fortalecen su posicionamiento y competitividad en el mercado.

Capítulo II: Fundamentos teóricos y conceptuales

Este capítulo expone las etapas necesarias para implementar la seguridad informativa en Corbantrade S.A.S., utilizando métodos organizados, respaldados por gráficos y herramientas visuales que mejoran la comprensión. Cada etapa tiene como meta garantizar la conformidad con las normas, reducir los riesgos y reforzar la protección de los activos de información.

2.1. Diagnóstico inicial y análisis de riesgos

El primer paso consiste en evaluar la situación actual de la empresa, lo que permite identificar las brechas de seguridad y establecer prioridades. Se considera tres etapas principales:

- **Levantamiento de inventario de activos de información**

Nuñez (2025) recomienda iniciar el diagnóstico con la identificación de activos críticos como servidores, sistemas y bases de datos.

- **Identificación de vulnerabilidades y amenazas**

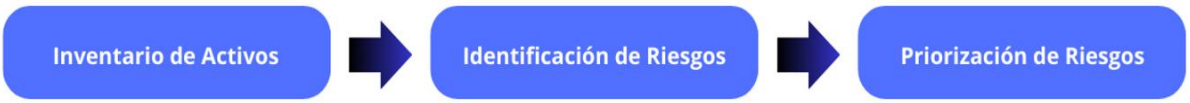
Como plantea Lema (2025), detectar vulnerabilidades internas y amenazas externas es esencial para ajustar de manera dinámica las medidas de seguridad.

- **Análisis de riesgos**

Según Santos Malpica (2023), evaluar la probabilidad e impacto de los incidentes permite priorizar los controles más relevantes y optimizar recursos en la gestión de riesgos.

La Figura 1 muestra que el diagnóstico inicial sigue un flujo lógico: empieza con el inventario de activos, prosigue con la detección de riesgos y concluye con su ordenación por prioridad.

Figura 13
Flujo del diagnóstico inicial de seguridad de la información en Corbantrade S.A.S.



Nota. Tomado de (Canva, 2025b)

2.2. Definición de políticas y roles de seguridad

Una vez identificado la situación actual y los riesgos de la empresa, el siguiente paso es oficializar las políticas internas y designar puestos de seguridad. Este procedimiento es esencial para que la organización tenga directrices definidas y responsabilidades establecidas:

- **Redacción de políticas internas**

Tal como mencionan Aguilar y Cuenca (2025), el desarrollo de políticas internas claras y documentadas constituye la base de un SGSI robusto, ya que facilita tanto la capacitación como las auditorías. En este sentido, Moscoso (2025) advierte que la falta de políticas y roles definidos incrementa los riesgos de incumplimiento normativo en el sector financiero.

- **Definición de responsables**

Según Nuñez (2025), un SGSI efectivo requiere que la organización designe un responsable formal y asigne funciones claras a cada área, con apoyo de la dirección y del departamento de TI, evitando duplicidades y vacíos en la gestión.

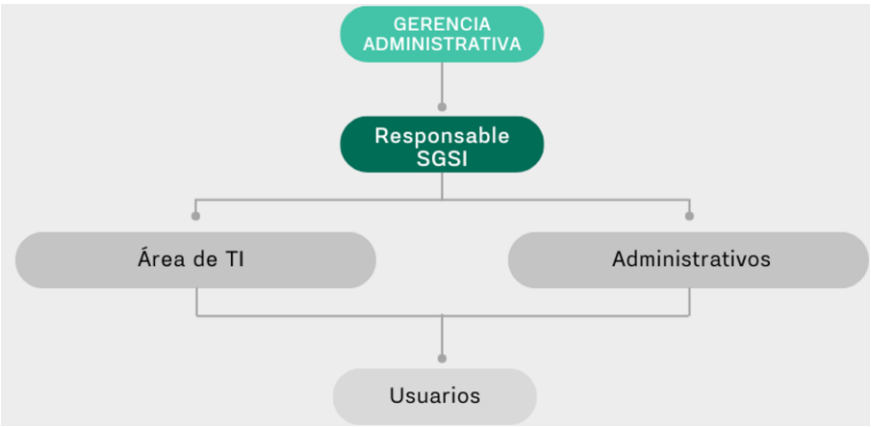
- **Asignación de responsabilidades claras**

De acuerdo con Verdugo (2023), la madurez en ciberseguridad de una organización depende en gran medida de la claridad en la asignación de roles y responsabilidades. Esto coincide con Aguilar y Cuenca (2025), quienes sostienen que la definición formal de responsabilidades garantiza la sostenibilidad de las medidas de seguridad.

Como se observa en la figura 2, los roles y las responsabilidades están organizados de manera jerárquica; los gerentes dirigen el proceso desde arriba y los usuarios finales siguen las reglas desde abajo.

Para proporcionar más detalles sobre el grado de participación de cada actor, se elaboró una tabla RACI (Tabla 1). Muestra quién es el responsable de ejecutar, quién está a cargo, quién colabora y quién debe ser informado sobre cada actividad clave del SGSI.

*Figura **14***
Organigrama de roles de seguridad de la información en Corbantrade S.A.S.



Nota. Tomado de (Canva, 2025e)

Tabla 2

Matriz RACI de roles y responsabilidades en la gestión de seguridad de la información en Corbantrade S.A.S.

Actividad	**Gerencia**	**Responsable SGSI**	**Área de TI**	**Administrativos**	**Usuarios**
Definición de políticas de seguridad	A	R	C	C	I
Gestión de accesos y contraseñas	I	A	R	C	C
Respaldo y recuperación de información	I	A	R	C	C
Identificación y análisis de riesgos	I	A	R	C	C
Capacitación y concienciación en seguridad	A	R	C	C	I
Monitoreo y auditoría interna	A	R	C	I	I
Respuesta a incidentes de seguridad	I	A	R	C	I

Nota. Adaptado al modelo RACI, donde R = Responsable, A = Aprueba o supervisa, C = Colabora y I = Informado

2.3. Selección e implementación de controles de seguridad

Tras la definición de roles y políticas internas, el siguiente paso consiste en la selección y aplicación de controles de seguridad que garanticen la protección de los activos de información. Estos controles deben elegirse de acuerdo con los riesgos identificados en la fase de diagnóstico, priorizando aquellos con mayor probabilidad de ocurrencia e impacto.

Los controles recomendados se inspiran en la norma ISO/IEC 27002, que ofrece un catálogo de buenas prácticas técnicas, administrativas y físicas. Entre los más relevantes para Corbantrade S.A.S. se encuentran:

- **Control de accesos**

Como señala Lema (2025), la implementación de controles debe responder al análisis de riesgos previo, priorizando aquellos con mayor impacto y probabilidad de ocurrencia.

- **Seguridad en la red y servidores**

De acuerdo con Aguilar y Cuenca (2025), los controles técnicos y administrativos propuestos en la norma ISO/IEC 27002 contribuyen a establecer procedimientos estandarizados que refuercen la seguridad de la información. Esto coincide con Yánez (2022), quien destaca que marcos como el NIST CSF (alineados a ISO) priorizan la protección y la respuesta ante incidentes.

- **Protección de datos**

Tal como advierte Morocho (2025), medidas como el cifrado de información sensible, la gestión de respaldos y el control de accesos son necesarias no solo como buenas prácticas, sino también como exigencias de la LOPDP.

- **Gestión de incidentes**

Procedimientos documentados para detectar, informar y reaccionar ante incidentes de seguridad.

- **Concienciación del personal**

En línea con Verdugo (2023), la concienciación del personal es un control indispensable para alcanzar la madurez en ciberseguridad, ya que fortalece la cultura organizacional frente a amenazas como el phishing.

En la tabla 2 hay un gráfico que contrasta los controles propuestos, sus metas y el área de la organización responsable de implementarlos.

Tabla 3

Controles de seguridad sugeridos para Corbantrade S.A.S.

Control de Seguridad	Objetivo principal	Responsable
Control de accesos	Restringir y monitorear el acceso a la información	Área TI Responsable SGSI
Firewall y segmentación VLAN	Proteger la red contra accesos no autorizados	Área TI
Cifrado y respaldos automáticos	Garantizar la integridad y disponibilidad de los datos	Área TI Administrativos
Procedimientos de incidentes	Responder de forma rápida y documentada a fallos o ataques	Responsable SGSI
Capacitación interna	Fortalecer la cultura de seguridad organizacional	Gerencia Área TI

2.4. Capacitación y sensibilización del personal

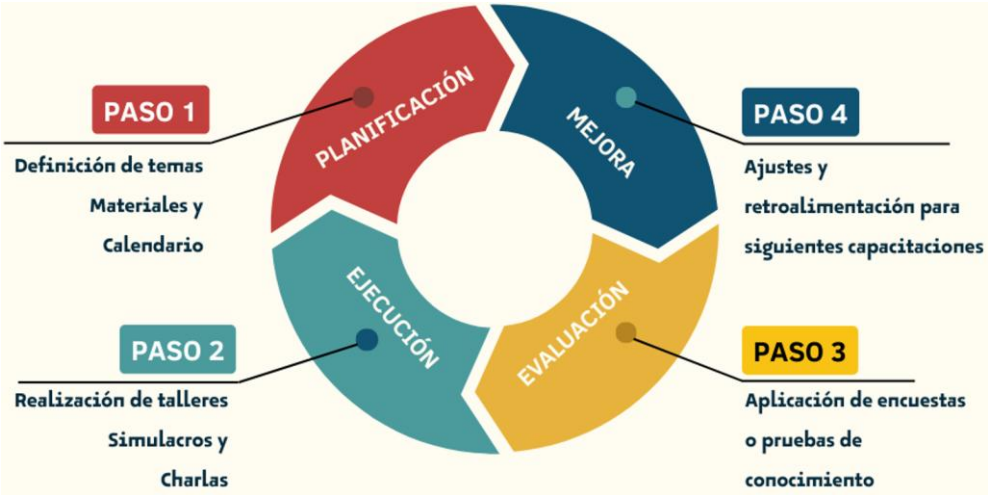
Un componente crucial para poner en práctica las políticas de seguridad de la información es la concienciación de los empleados. Si no comprenden la importancia de proteger la información y no siguen las buenas prácticas en su trabajo diario, los controles técnicos son insuficientes.

Se recomienda que Corbantrade S.A.S. establezca un programa de formación continua para todos los empleados. Este programa debería incluir:

- Charlas y talleres prácticos sobre cómo manejar correctamente las contraseñas, utilizar el correo electrónico de forma segura y reconocer los intentos de phishing.
- Simulaciones de incidentes de seguridad, como evaluaciones de la preparación de los empleados ante ciberataques.
- Directrices claramente definidas para el uso de dispositivos y recursos tecnológicos que sean fáciles de comprender y distribuir.
- Campañas de concienciación internas que promuevan las mejores prácticas a través de boletines informativos, infografías o comunicaciones internas.
- Evaluaciones frecuentes para medir los conocimientos adquiridos y modificar la formación en función de los resultados.
- Implementación de contraseñas.

Las distintas fases del programa de formación en seguridad de la información sugerido para Corbantrade S.A.S. se describen en la figura 3.

Figura 15
Fases del programa de capacitación en seguridad de la información.



Nota. Tomado de (Canva, 2025c)

Como parte de la conexión con la sociedad, se organizó una charla para concienciar al personal administrativo y técnico de Corbantrade S.A.S., en la que se compartieron las normas básicas para la seguridad de la información. En la figura 4 se muestra un ejemplo de esta actividad, y en el anexo 5 se incluyen todas las fotografías que dan fe de su celebración.

Figura 16
Charla de sensibilización en seguridad de la información al personal de Corbantrade S.A.S.

2.5. Monitoreo, auditoría y mejora continua

El éxito de un Sistema de Gestión de Seguridad de la Información (SGSI) depende de su habilidad para ser evaluado y mejorado continuamente. En Corbantrade S.A.S., este procedimiento debe abarcar tres ejes centrales:

- **Monitoreo constante**

Control de sucesos reportados, verificación de accesos y supervisión del acatamiento de las políticas.

- **Auditoría interna**

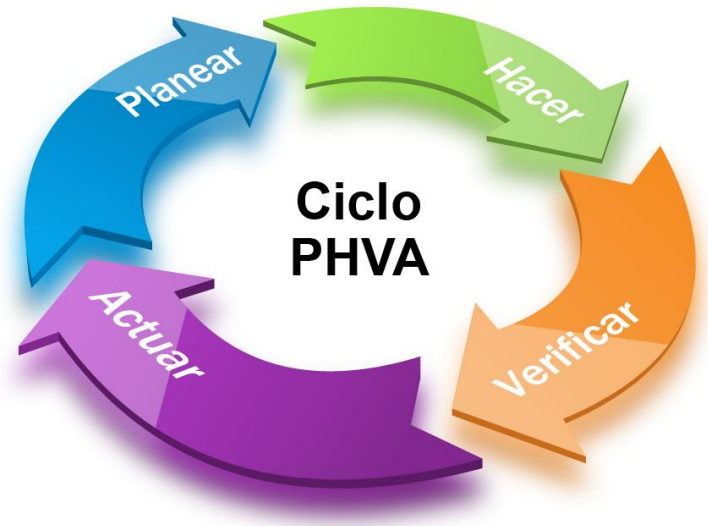
Exámenes regulares para analizar el grado de cumplimiento de la LOPDP y la norma ISO/IEC 27001:2022, comprobando la eficacia de los controles que se han implementado.

- **Mejora continua**

Modificaciones a las políticas y procesos en función de los hallazgos de auditoría, nuevas amenazas o alteraciones tecnológicas.

Como se ilustra en la Figura 5, el ciclo PHVA (Planificar, Ejecutar, Verificar y Actuar) es compatible con el SGSI de Corbantrade S.A.S. Se encarga de organizar las etapas de planificación de políticas, implementación de controles, verificación mediante auditorías y actualización continua para mejorar el sistema de seguridad de la información.

Figura 17
Ciclo PHVA aplicado al monitoreo y mejora continua del SGSI en Corbantrade S.A.S.



Nota. Tomado de (Correa, 2022)

2.6. Casos de aplicación en Corbantrade S.A.S.

La puesta en marcha de un Sistema de Gestión de Seguridad de la Información (SGSI) no debe limitarse a ser teórica; requiere ejemplos prácticos que evidencien su aplicabilidad en la organización. Se muestran ejemplos de aplicación que reflejan medidas de seguridad concretas, adaptadas a la realidad de Corbantrade S.A.S.:

- **Gestión de contraseñas seguras**

Se sugiere implementar una política que exija a todos los usuarios modificar sus contraseñas cada 90 días, con parámetros de complejidad establecidos (mínimo 12 caracteres, combinación de letras, números y símbolos). Esto contribuiría a reducir el riesgo de accesos no autorizados.

- **Respaldo y recuperación de la información contable**

Se recomienda establecer un sistema de copias de seguridad automáticas diarias en un servidor secundario, además de copias cifradas en la nube cada semana. Esto garantizaría que los procesos continuaran operando pese a que la infraestructura local sufriera una falla crítica.

- **Simulacro de intento de phishing**

Se aconseja realizar simulacros de correos electrónicos fraudulentos durante la formación del personal para observar cómo reaccionan los trabajadores. Los resultados facilitarían la modificación de las capacitaciones, para que puedan ajustarse a las debilidades detectadas.

- **Auditoría interna**

Se sugiere que las auditorías internas verifiquen si se están cumpliendo con las políticas de seguridad. Si encuentran algún problema (como, por ejemplo, con la forma en que se registran los incidentes), deben crear formularios estandarizados para documentar y darle seguimiento a cada caso; tal como recomienda Lema (2025), priorizando controles y asegurando la mejora continua del SGSI.

Estos casos, que aparecen en la Tabla 3, abarcan la administración de contraseñas seguras, los métodos de respaldo de datos contables, las simulaciones de intentos de phishing y las auditorías internas. La finalidad es brindarle a la organización un marco práctico para reforzar la seguridad de la información y garantizar que las operaciones sigan funcionando, por lo cual cada caso incluye la medida recomendada y el beneficio esperado.

Tabla 4

Casos de aplicación propuestos en Corbantrade S.A.S.

Caso	Medida Propuesta	Beneficio Esperado
Gestión de contraseñas seguras	Implementar una política que obligue a cambiar las contraseñas cada 90 días, con requisitos de complejidad (mínimo 12 caracteres, combinación de letras, números y símbolos).	Reducir el riesgo de accesos no autorizados a los sistemas internos y proteger datos sensibles de clientes y de la organización.
Respaldo y recuperación de información contable	Configurar respaldos automáticos diarios en un servidor secundario y copias semanales cifradas en la nube.	Garantizar la continuidad operativa y evitar pérdida de información crítica en caso de fallas o incidentes.
Simulación de intento de phishing	Realizar simulacros de correos fraudulentos para evaluar la capacidad de respuesta del personal y reforzar la capacitación.	Incrementar la conciencia de seguridad de los empleados y reducir la probabilidad de caer en fraudes electrónicos.
Auditoría interna	Verificar en auditorías periódicas el cumplimiento de políticas y formalizar registros estandarizados de incidentes.	Mejorar la trazabilidad de los incidentes de seguridad y fortalecer la cultura de cumplimiento normativo.

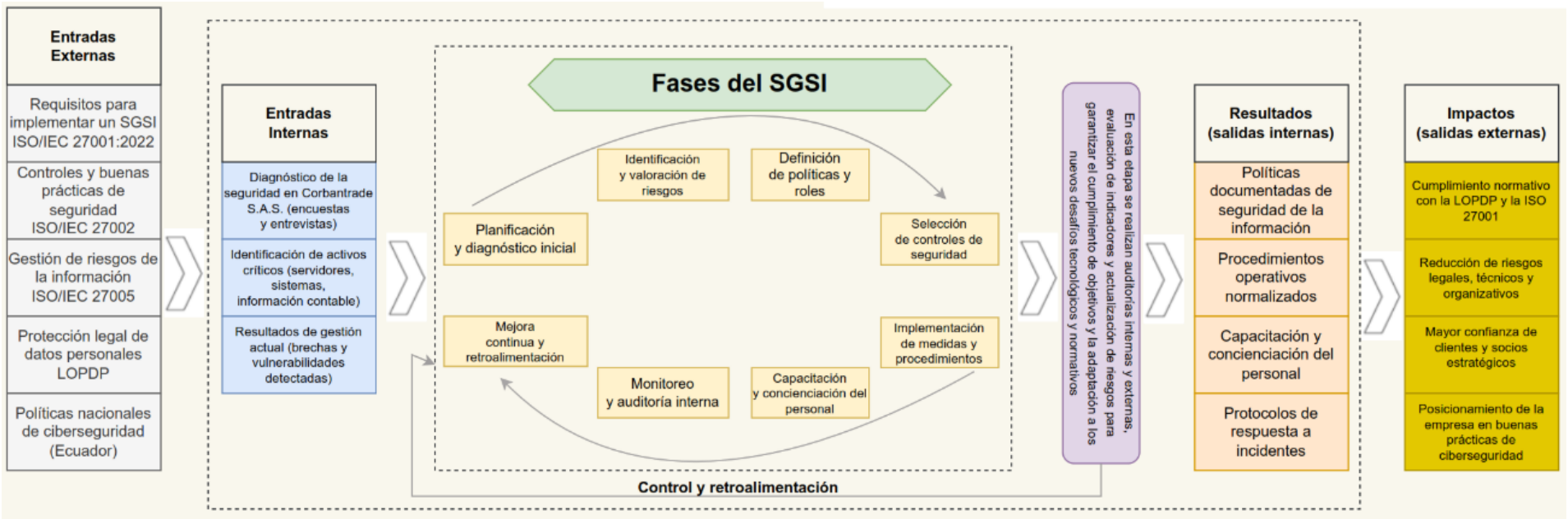
Nota. Esta tabla presenta casos de aplicación propuestos para Corbantrade S.A.S., los cuales sirven como referencia práctica en la implementación de la guía.

Después de finalizar las etapas señaladas, es posible resumir la ejecución del SGSI en un modelo completo que incluye los ingresos externos (normas, leyes y políticas nacionales), los ingresos internos (diagnóstico y brechas detectadas), las fases del sistema (planificación, políticas, controles, capacitación, supervisión y mejora continua) y también los resultados e impactos previstos (cumplimiento normativo, reducción de riesgos, confianza del cliente y fortalecimiento de la cultura organizacional).

El concepto se ilustra de manera sencilla en la figura 6, que muestra cómo cada elemento está vinculado en un ciclo de retroalimentación constante.

Figura 18

Modelo integral de implementación del SGSI en Corbantrade S.A.S.



Capítulo III: Herramientas o Recursos Complementarios

La efectividad de un Sistema de Gestión de Seguridad de la Información (SGSI) no depende solo del establecimiento de controles y políticas, sino también del suministro de recursos útiles que hagan posible su aplicación en el día a día. Para facilitar la implementación de las medidas propuestas y asegurar que todos los empleados puedan comprender, verificar y acceder a los procesos de seguridad, este capítulo incluye herramientas de apoyo creadas para Corbantrade S.A.S.

Estos recursos abarcan plantillas y formatos para documentar las actividades esenciales de seguridad, listas de control que posibilitan evaluar el seguimiento de buenas prácticas, así como también materiales gráficos (infografías y diagramas) que facilitan la comprensión de los procedimientos.

3.1. Formatos y plantillas

Se sugieren formatos y plantillas para simplificar el control y la grabación de procesos clave, garantizando trazabilidad y consistencia en la gestión de seguridad de la información. Estos documentos estandarizados son esenciales para cumplir con la exigencia de un SGSI de documentar procedimientos y registros (Aguilar & Cuenca, 2025). Uno de los más relevantes es el Registro de Incidentes de Seguridad, práctica alineada con lo establecido en la norma ISO/IEC 27001:2022, ya que permite registrar y dar tratamiento formal a sucesos que afectan la confidencialidad, integridad o disponibilidad de la información (Moscoso, 2025).

Uno de los formatos más relevantes es el Registro de Incidentes de Seguridad, ya que brinda la posibilidad de registrar sistemáticamente los sucesos que impactan o tienen el potencial de impactar la confidencialidad, integridad o disponibilidad de la información. Este registro se utiliza para auditorías internas, análisis de riesgos y procesos de mejora continua.

El Registro de Incidentes de Seguridad, que posibilita mantener un registro organizado de los sucesos que comprometen o pueden comprometer la confidencialidad, integridad o disponibilidad de la información, es uno de los formatos más relevantes. El Cuadro 4 presenta una muestra que Corbantrade S.A.S. podría desear utilizar.

Tabla 5

Formato de Registro de Incidentes de Seguridad en Corbantrade S.A.S.

Fecha	Tipo de incidente	Descripción del evento	Impacto estimado	Acciones correctivas	Responsable	Estado
dd/mm/aaaa	Acceso no autorizado	Usuario externo intentó ingresar al sistema contable	Alto	Bloqueo de IP y refuerzo de autenticación	Área TI	Cerrado
dd/mm/aaaa	Pérdida de información	Carpeta compartida eliminada accidentalmente	Medio	Recuperación desde respaldo	Área TI	Resuelto
dd/mm/aaaa	Phishing detectado	Correo fraudulento enviado a personal administrativo	Bajo	Capacitación y filtrado de correos	Área administrativa	En proceso

Nota. Este formato es un ejemplo sugerido para Corbantrade S.A.S. y puede adaptarse de acuerdo con la naturaleza de los incidentes que se presenten en la organización.

La matriz de riesgos simplificada es una herramienta adicional útil que le ayuda a identificar los activos críticos, las amenazas que los afectan y el establecimiento de controles según el grado de impacto y probabilidad. En la tabla 5 se muestra un modelo útil que se ha modificado para satisfacer los requisitos de Corbantrade S.A.S.

Tabla 6
Matriz de riesgos simplificada para Corbantrade S.A.S.

Activo	Amenaza/Vulnerabilidad	Probabilidad	Impacto	Nivel de riesgo	Medida de control
Servidor de base de datos	Acceso no autorizado por credenciales débiles	Alta	Alto	Crítico	Implementar doble factor de autenticación y políticas de contraseñas seguras
Archivos contables compartidos	Eliminación accidental por usuario interno	Media	Alto	Alto	Configuración de respaldos automáticos diarios
Red corporativa	Intrusión externa mediante malware	Media	Alto	Alto	Uso de firewall corporativo y antivirus actualizado
Información de clientes	Phishing dirigido al personal administrativo	Alta	Medio	Alto	Capacitación continua y filtrado de correos sospechosos
Servidor de aplicaciones	Fallo eléctrico prolongado	Baja	Alto	Medio	Uso de UPS y políticas de respaldo en la nube

Nota. Ejemplo simplificado para Corbantrade S.A.S., siguiendo criterios básicos de probabilidad e impacto. Puede ser ampliada con metodologías más completas como ISO/IEC 27005, OCTAVE o MAGERIT según el nivel de madurez de la organización.

Otro elemento crucial en la gestión de la seguridad de la información es el control de acceso. Solo las personas autorizadas pueden acceder a los recursos vitales de la empresa gracias a la gestión de usuarios, permisos y privilegios. Para cumplir con la norma ISO/IEC 27001:2022 y la LOPDP, Corbantrade S.A.S. debe disponer de un registro de acceso formal.

El formato de control de acceso que se muestra en la tabla 6 es un ejemplo que permite monitorear a quién tiene acceso a cada sistema, qué nivel de privilegio posee y cuándo dicho acceso deja de ser válido.

Tabla 7
Formato de control de accesos en Corbantrade S.A.S.

Nombre del usuario	Área/Departamento	Sistema o recurso	Nivel de acceso	Fecha de autorización	Responsable de aprobación	Estado
Juan Pérez	Contabilidad	Sistema contable (Dynamics)	Lectura/Escritura	15/01/2025	Jefe de TI	Activo
María López	Administración	Servidor de archivos	Solo lectura	20/01/2025	Responsable SGSI	Activo
Carlos Ruiz	TI	Firewall corporativo	Administrador	05/02/2025	Dirección General	Activo
Ana Torres	Finanzas	Base de datos clientes	Lectura	08/02/2025	Jefe de TI	Suspendido

Nota. Este formato es una herramienta práctica para Corbantrade S.A.S., ya que permite controlar el ciclo de vida de los accesos y detectar a tiempo cuentas inactivas, privilegios excesivos o inconsistencias en la gestión de usuarios.

3.2. Listas de verificación (checklists)

Las listas de verificación constituyen instrumentos eficaces para asegurar que las medidas de seguridad se apliquen de forma consistente y completa. Además, la norma ISO/IEC 27001:2022 establece la necesidad de realizar revisiones periódicas que garanticen la trazabilidad y mejora continua de los controles. En la misma línea, Nuñez (2025) sugiere que herramientas prácticas como los checklists permiten a las pymes implementar de manera gradual un SGSI adaptado a su contexto. Asimismo, Catota (2025) enfatiza que, en cumplimiento de la LOPDP, estas verificaciones deben efectuarse de forma periódica para reducir riesgos legales y técnicos.

Una lista de verificación básica para la seguridad que deben utilizar el área de TI y los encargados de procesos fundamentales está presentada en la Tabla 7.

Tabla 8
Lista de verificación básica de seguridad en Corbantrade S.A.S.

Ítem de verificación	**Cumple (Sí/No)**	**Observaciones**
¿Existen copias de seguridad actualizadas y verificadas?		
¿Se aplican políticas de contraseñas seguras?		
¿Los accesos de usuarios inactivos han sido eliminados?		
¿Se han actualizado los sistemas y aplicaciones críticas?		
¿Se realizan simulacros de incidentes de seguridad?		
¿El personal ha recibido capacitación en el último año?		

Nota. Este checklist puede aplicarse de forma trimestral en Corbantrade S.A.S. para evaluar el cumplimiento de las medidas de seguridad básicas y generar reportes de seguimiento.

Las entidades, además de las medidas técnicas, tienen que garantizar la observancia de la Ley Orgánica de Protección de Datos Personales (LOPDP). Este marco legal define las obligaciones relacionadas con la manipulación, protección y custodia de datos personales. La Tabla 8 contiene una enumeración de acciones que la empresa tiene que llevar a cabo para cumplir con la LOPDP. Esto posibilita determinar si la compañía está utilizando los principios legales apropiados al gestionar la información.

Tabla 9

Lista de verificación de cumplimiento con la LOPDP en Corbantrade S.A.S.

Ítem de verificación (LOPDP)	**Cumple (Sí/No)**	**Observaciones**
¿Se informa a los titulares sobre el uso de sus datos personales?		
¿Existen políticas internas documentadas sobre protección de datos?		
¿Se aplica el principio de minimización (solo datos necesarios)?		
¿Se cuenta con mecanismos para el ejercicio de derechos ARCO?		
¿Los contratos con proveedores incluyen cláusulas de protección de datos?		
¿Se han implementado medidas técnicas de seguridad (cifrado, accesos)?		
¿Se realizan auditorías o revisiones periódicas de cumplimiento?		

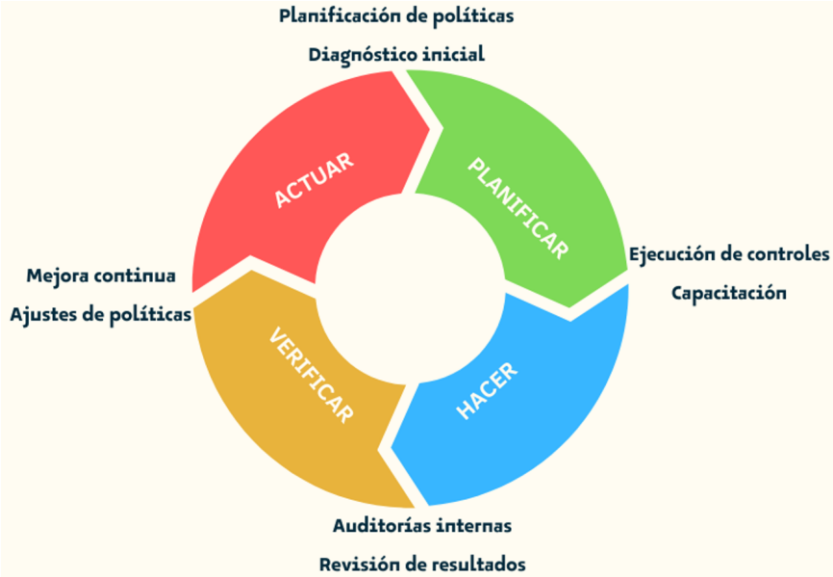
Nota. Esta lista de verificación ayuda a Corbantrade S.A.S. a cumplir con los principios de legalidad, transparencia, proporcionalidad y responsabilidad proactiva establecidos en la LOPDP, puede ser revisada semestralmente.

3.3. Infografías y diagramas prácticos

La representación visual de los procesos mediante infografías y diagramas facilita la comprensión y aplicación de las políticas de seguridad. Según Aguilar y Cuenca (2025), los esquemas gráficos son un componente clave en la documentación de un SGSI, pues fortalecen la cultura de seguridad organizacional. De igual manera, Yánez (2022) sostiene que los recursos visuales adaptados al contexto de cada institución hacen que los marcos internacionales sean más accesibles para los usuarios. En este sentido, Verdugo (2023) enfatiza que las pymes requieren diagramas claros que traduzcan la complejidad de la normativa en pasos concretos y aplicables.

La figura 7 muestra el Ciclo PHVA (Planificar, Hacer, Verificar, Actuar) aplicado al Sistema de Gestión de Seguridad de la Información (SGSI) de Corbantrade S.A.S. Muestra cómo las fases se colaboran en un proceso de mejora continua.

Figura *19*
Ciclo PHVA aplicado al SGSI en Corbantrade S.A.S.



Nota. Tomado de (Canva, 2025d)

Además del ciclo PHVA, es esencial concebir la seguridad como un modelo por capas, en el que cada capa protege a las demás. La figura 8 presenta las capas de seguridad que se han propuesto para Corbantrade S.A.S, que van desde la protección física hasta la capacitación para los usuarios.

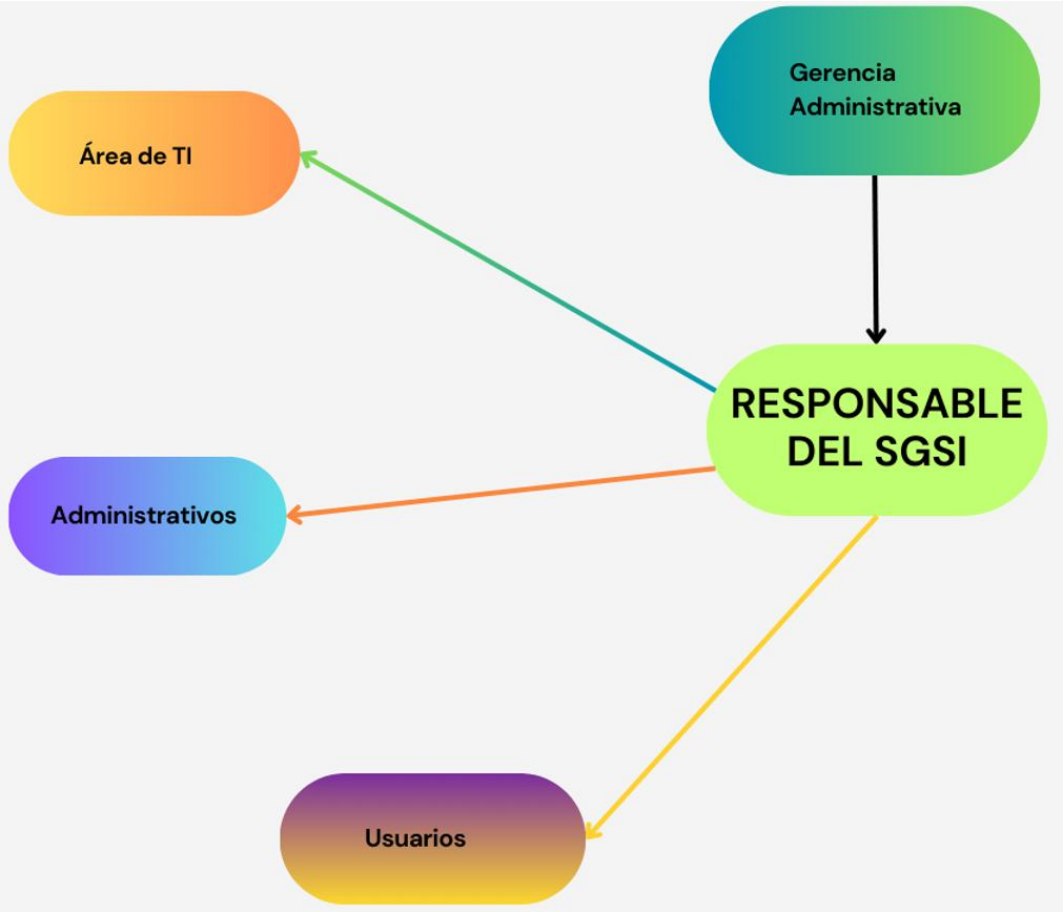
Figura 20
Esquema de capas de seguridad en Corbantrade S.A.S.

Nota. Tomado de (Canva, 2025a)

En la figura 9 se muestra un mapa de los actores y las responsabilidades en materia de seguridad de la información. En él se muestra cómo colaboran los distintos niveles organizativos. A diferencia del organigrama jerárquico (figura 2), este diagrama hace mayor hincapié en la colaboración y la comunicación entre todos los componentes del SGSI.

Figura 21

Mapa de actores y responsabilidades en seguridad de la información.



Nota. Tomado de (Canva, 2025f)

3.4. Recomendaciones para la implementación

Los formularios, listas de verificación e infografías creados en este capítulo deben incorporarse a las operaciones diarias de la empresa para que se utilicen correctamente. Para ello, se ofrecen las siguientes recomendaciones: estas herramientas deben ser adoptadas como parte de la cultura organizacional y no verse únicamente como documentos aislados. Además, se recomienda designar responsables para su actualización y asegurar que cada recurso tenga un proceso de revisión continua que garantice su vigencia frente a cambios tecnológicos y regulatorios:

- **Integración en la gestión organizacional**

Los instrumentos deben integrarse en los procesos rutinarios de Corbantrade S.A.S., en lugar de utilizarse como actividades independientes. Esto significa que las listas de verificación se utilizan en auditorías internas, los formatos de riesgo se utilizan para crear informes mensuales y los diagramas se utilizan para apoyar la formación.

- **Actualización periódica**

Al menos una vez al año o después de cada incidente de seguridad, se deben revisar todos los documentos (plantillas, listas de verificación y gráficos) para garantizar que reflejan las nuevas amenazas, normativas o avances tecnológicos.

- **Accesibilidad para los usuarios**

Los recursos deben estar disponibles en un repositorio interno compartido (como una intranet o un servidor de archivo) para que cualquier miembro del personal pueda acceder a ellos y utilizarlos fácilmente.

- **Uso en capacitaciones**

Se recomienda incluir estos recursos en campañas de sensibilización y cursos de formación continua. Las infografías y los diagramas ayudan a las personas a comprender y retener mejor los conceptos.

- **Validación mediante auditorías**

La eficacia debe evaluarse mediante auditorías internas y externas del SGSI, registrando los resultados y mejorando continuamente el material.

Con la ayuda de estas sugerencias, los recursos creados se transforman de meros instrumentos teóricos en herramientas útiles que pueden utilizarse para mejorar la cultura de ciberseguridad de la empresa y garantizar el cumplimiento de la norma ISO/IEC 27001:2022 y la LOPDP.

Capítulo IV: Buenas prácticas y consideraciones finales

En este capítulo se recogen las principales sugerencias para garantizar la implementación eficiente, duradera y flexible del Sistema de Gestión de Seguridad de la Información (SGSI) en Corbantrade S.A.S. A diferencia de los capítulos anteriores, que se centraban en prácticas y recursos concretos, este capítulo hace hincapié en los elementos generales que contribuyen al desarrollo de una cultura de seguridad en el lugar de trabajo.

El objetivo es que la organización no solo implemente controles técnicos y organizativos, sino que también aprenda de los errores comunes, mejore sus procesos mediante buenas prácticas y mantenga una perspectiva estratégica centrada en el éxito del SGSI.

4.1. Errores comunes que se deben evitar

Las organizaciones se enfrentan con frecuencia a problemas que reducen la eficacia de los Sistemas de Gestión de la Seguridad de la Información (SGSI) cuando los implementan. Los errores más frecuentes detectados en procedimientos comparables se enumeran en la tabla 9, junto con una breve descripción de cómo afectan a la gestión de la seguridad de la información.

Tabla *10*
Errores comunes en la implementación de un SGSI

Error común	Descripción
Ausencia de apoyo de la alta dirección	Un SGSI no puede sostenerse si la gerencia no se compromete activamente. La falta de liderazgo provoca que las políticas queden solo en documentos sin aplicación práctica.
No involucrar al personal	Considerar la seguridad de la información como un asunto exclusivo del área de TI es un error frecuente. Si los colaboradores no son parte activa del proceso, las políticas se incumplen y los riesgos aumentan.
Falta de actualización continua	Implementar un SGSI y dejarlo sin revisiones periódicas lo convierte en un sistema obsoleto. Los riesgos evolucionan constantemente, y si no se actualizan los controles, se crean brechas de seguridad.
Enfoque excesivo en la parte técnica	Limitar el SGSI solo a firewalls, antivirus o servidores, sin considerar procesos, roles y políticas organizacionales, lleva a un sistema incompleto y poco sostenible.

Deficiente gestión documental	No contar con manuales, políticas y procedimientos claramente definidos impide medir el cumplimiento y dificulta las auditorías internas o externas.
Falta de indicadores de seguimiento	Sin métricas claras (ejemplo: número de incidentes reportados, tiempo de respuesta, porcentaje de cumplimiento de capacitación), es imposible evaluar la efectividad del sistema.

4.2. Sugerencias para una implementación exitosa

Para que un Sistema de Gestión de Seguridad de la Información (SGSI) opere con eficacia, es indispensable implementar prácticas que aseguren su sostenibilidad y aceptación en el seno de la entidad. La Tabla 8 ilustra las recomendaciones más relevantes que incrementan las probabilidades de que el SGSI funcione en Corbantrade S.A.S.

Tabla *11*
Sugerencias para una implementación exitosa de un SGSI.

Sugerencia	Descripción
Compromiso de la alta dirección	Garantizar que la gerencia respalde el SGSI con recursos, liderazgo visible y toma de decisiones alineadas con la seguridad de la información.
Involucrar a todo el personal	Fomentar la participación de colaboradores en todas las áreas mediante programas de capacitación, campañas de concienciación y retroalimentación continua.
Actualización constante	Revisar y actualizar periódicamente las políticas, procedimientos y controles de seguridad para adaptarlos a los cambios tecnológicos y normativos.
Enfoque integral	Considerar no solo los aspectos técnicos, sino también los organizativos, legales y humanos que forman parte del ecosistema de seguridad.
Gestión documental organizada	Mantener manuales, políticas y procedimientos claros y accesibles para todo el personal, facilitando la trazabilidad y las auditorías.

Definir indicadores de desempeño	Establecer métricas claras (ejemplo: número de incidentes, tiempo medio de respuesta, nivel de cumplimiento en capacitaciones) para evaluar la efectividad del SGSI.

4.3. Factores de éxito en la gestión de seguridad de la información

La implementación y la sostenibilidad de un Sistema de Gestión de Seguridad de la Información (SGSI) no se basan solamente en establecer controles técnicos, sino también en varios elementos estratégicos y organizativos. Los elementos que determinan el grado de madurez y eficacia del sistema en Corbantrade S.A.S. se sintetizan en la Tabla 11.

Tabla 12
Factores de éxito en la gestión de seguridad de la información

Factor de éxito	Descripción
Apoyo continuo de la alta dirección	El liderazgo debe comprometerse con recursos, presupuesto y respaldo estratégico al SGSI.
Cultura organizacional de seguridad	Fomentar hábitos y prácticas seguras en todos los niveles de la organización, integrando la seguridad en la rutina laboral.
Capacitación permanente	Actualizar constantemente al personal sobre amenazas, normativas y procedimientos internos.
Gestión proactiva de riesgos	Identificar y priorizar riesgos de manera preventiva, antes de que generen incidentes.
Mejora continua (PHVA)	Mantener un ciclo constante de planificación, ejecución, verificación y ajuste de las políticas y controles de seguridad.
Comunicación efectiva	Hay que asegurar que las políticas, procedimientos y cambios sean conocidos por todo el personal en un lenguaje claro y accesible.
Medición de resultados	Utilizar indicadores clave (KPIs) para evaluar la efectividad del SGSI y tomar decisiones basadas en evidencias.

CONCLUSIONES Y RECOMENDACIONES

Conclusiones

Esta guía es una herramienta útil para ayudar a Corbantrade S.A.S. a mejorar la seguridad de la información de acuerdo con las normas ISO/IEC 27001:2022 y LOPDP. Su desarrollo demostró que una gestión eficaz de la seguridad requiere no solo medidas técnicas, sino también políticas claras, formación de los empleados y un compromiso de alto nivel.

En términos generales, la guía ofrece un marco estructurado que puede aplicarse dentro de la organización y replicarse en otras empresas financieras y responsables. El objetivo es fomentar una cultura organizativa que gestione eficazmente los riesgos y proteja los datos, lo que respaldará las operaciones de la empresa y el cumplimiento de la normativa establecida.

Recomendaciones

Se recomienda que la guía siga siendo un documento vivo que se actualice con frecuencia con nuevas técnicas y salvaguardias para hacer frente a los riesgos emergentes. Además, se recomienda mejorar esta propuesta mediante:

- Auditorías internas y externas que permitan evaluar la verdadera eficacia de los controles implementados.
- La inclusión de métricas inequívocas (KPI) que faciliten el seguimiento de los efectos de la SGSI a lo largo del tiempo.
- La integración con marcos internacionales adicionales, como el Marco de Ciberseguridad del NIST o el Modelo de Madurez de Ciberseguridad (C2M2), lo que ampliaría la visión de la empresa y reforzaría su competitividad.

En resumen, esta guía debe considerarse como una base que establece el marco para una gestión eficaz de la seguridad de la información; sin embargo, debe ampliarse con procedimientos para la innovación continua, la mejora y la disposición a absorber los conocimientos de otros.

REFERENCIAS BIBLIOGRÁFICAS

Aguilar, C., & Cuenca, J. (2025). Diseño de un sistema de gestión de seguridad de la información (SGSI) basado en el estándar ISO/IEC 27001 para la empresa EJEPROY CIA. LTDA. *MQRInvestigar* , *9*(1), e361. https://doi.org/10.56048/MQR20225.9.1.2025.e361

Canva. (2025a). *Capas de seguridad*. https://www.canva.com/design/DAGxekkLVZI/1OOYPdHD4SteK9jJggoDyA/edit?ui=eyJBIjp7fX0

Canva. (2025b). *Flujo del diagnóstico inicial de seguridad de la información*. https://www.canva.com/design/DAGxYz_u47Y/sKADadgWvYEOW4D0M96W_Q/edit?referrer=flowcharts-landing-page

Canva. (2025c). *Gráfico de etapas seguridad*. https://www.canva.com/design/DAGxej5GFTA/u4qSaj3UcCfurHqtpg-_lw/edit

Canva. (2025d). *Gráfico del ciclo PHVA*. https://www.canva.com/design/DAGxZlGODjk/HmDKiL5PO_aTFt6pOpjF4g/edit

Canva. (2025e). *Gráfico Organigrama roles de seguridad de la información*. https://www.canva.com/design/DAGxZItmhwU/ND19LPtb_UiDAR-pAqGvlQ/edit

Canva. (2025f). *Mapa de actores y responsabilidades en seguridad de la información*. https://www.canva.com/design/DAGxeiM8vqw/fCH8nZ6TCQyY4vzJ1UOI7A/edit?ui=eyJBIjp7fX0

Catota, A. (2025). *PROPUESTA DE UNA MEJORA DE LA SEGURIDAD DE LA INFORMACIÓN EN UN NEGOCIO FIDUCIARIO DANDO CUMPLIMIENTO A LA LEY DE PROTECCIÓN DE DATOS PERSONALES EN EL ECUADOR USANDO UNA PRUEBA DE CONCEPTO Y PROPONIENDO UNA CONTRAMEDIDA*.

Correa, E. (2022, March 8). *CÓMO APLICAR UNA ESTRATEGIA PHVA EXITOSA*. https://www.linkedin.com/pulse/c%C3%B3mo-aplicar-una-estrategia-phva-exitosa-edgar-g-/

Lema, oscar. (2025). *Propuesta de un sistema de seguridad de la información para una Empresa de Telecomunicaciones bajo la Norma ISO/IEC 27005*. http://repositorio.uisrael.edu.ec/bitstream/47000/4305/1/UISRAEL-EC-MASTER-SEG-INF-PRO-378.242-2025-004.pdf

Morocho, C. (2025). *Buenas prácticas para el cumplimiento de la Ley de Protección de Datos Personales en el Sistema Nacional de Rendición de Cuentas bajo las Normas ISO/IEC 27001*. http://repositorio.uisrael.edu.ec/bitstream/47000/4309/1/UISRAEL-EC-MASTER-SEG-INF-PRO-378.242-2025-008.pdf

Moscoso, J. (2025). *"EVALUACIÓN JURÍDICA DE RIESGOS Y VULNERABILIDADES EN LA PROTECCIÓN DE DATOS EN INSTITUCIONES FINANCIERAS DEL ECUADOR BAJO LA LEY ORGÁNICA DE PROTECCIÓN DATOS PERSONALES."* https://dspace.ucacue.edu.ec/server/api/core/bitstreams/de4b613c-519b-4f9c-9852-8d18ac21e733/content

Nuñez, D. (2025). *Modelo para la Gestión de Seguridad de la Información en Cooperativas de Ahorro y Crédito del Segmento 1 Basada en ISO/IEC 27001:2022*. http://repositorio.uisrael.edu.ec/bitstream/47000/4312/1/UISRAEL-EC-MASTER-SEG-INF-PRO-378.242-2025-011.pdf

Romero, I. (2024). *CUMPLIMIENTO DE LA NORMATIVA DE SEGURIDAD DE LA INFORMACIÓN, PARA LA COAC ACHIK INTI DEL CANTÓN CAÑAR, SEGMENTO 4 Y SU PROGRESIÓN AL SEGMENTO 3, BAJO LA REGULACIÓN DE LA SEPS.*

Santos Malpica, I. (2023). *CTFs como medio de aprendizaje en la ciberseguridad*. Universidad Nacional de Educación a Distancia (España). Escuela Técnica Superior de Ingeniería Informática. https://e-spacio.uned.es/entities/publication/4a959d7c-2b9b-4a7d-acbc-e17d3f06e795

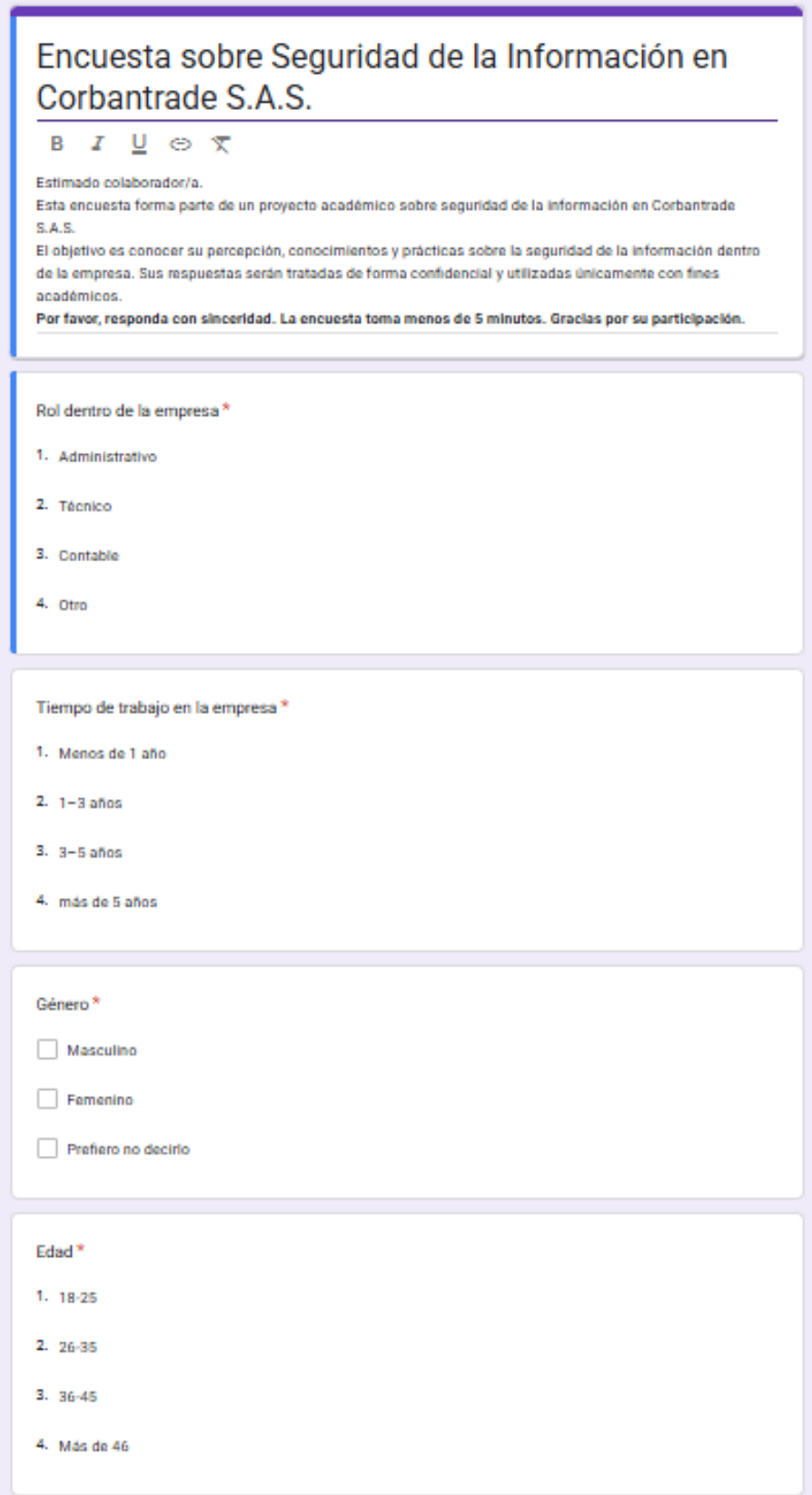
Verdugo, G. (2023). *"PROPUESTA DE UN MODELO DE MADUREZ DE CIBERSEGURIDAD PARA ECUADOR."* https://dspace.ucacue.edu.ec/server/api/core/bitstreams/bb62d854-ad21-4ef0-ac9e-2731ba7ea16c/content

Yagual, G. (2024). *DESARROLLO DE UNA GUÍA DE IMPLEMENTACIÓN DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (SGSI) PARA EL DEPARTAMENTO DE SISTEMAS DEL GAD MUNICIPAL DE LA LIBERTAD*.

Yánez, J. (2022). *APLICACIÓN DEL "NIST CYBERSECURITY FRAMEWORK" EN EL INSTITUTO SUPERIOR TECNOLÓGICO "SUCRE."* https://repositorio.puce.edu.ec/server/api/core/bitstreams/1db0ae0e-c10e-4a07-8e19-4c721d726eec/content

ANEXOS

ANEXO 1



Encuesta sobre Seguridad de la Información en Corbantrade S.A.S.

Estimado colaborador/a.
Esta encuesta forma parte de un proyecto académico sobre seguridad de la información en Corbantrade S.A.S.
El objetivo es conocer su percepción, conocimientos y prácticas sobre la seguridad de la información dentro de la empresa. Sus respuestas serán tratadas de forma confidencial y utilizadas únicamente con fines académicos.
Por favor, responda con sinceridad. La encuesta toma menos de 5 minutos. Gracias por su participación.

Rol dentro de la empresa *

1. Administrativo
2. Técnico
3. Contable
4. Otro

Tiempo de trabajo en la empresa *

1. Menos de 1 año
2. 1–3 años
3. 3–5 años
4. más de 5 años

Género *

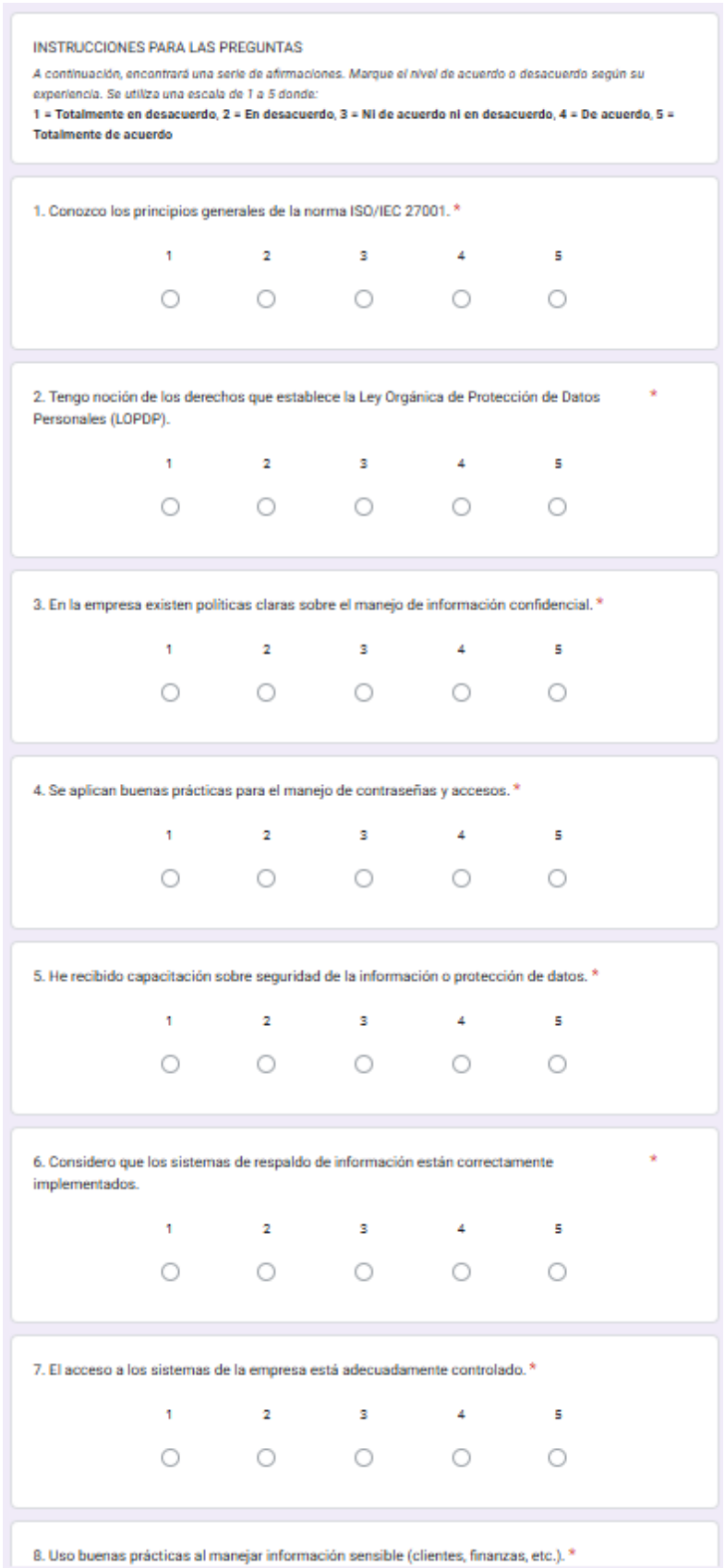
- [ ] Masculino
- [ ] Femenino
- [ ] Prefiero no decirlo

Edad *

1. 18-25
2. 26-35
3. 36-45
4. Más de 46

FORMATO DE ENCUESTA

ANEXO 2



INSTRUCCIONES PARA LAS PREGUNTAS

A continuación, encontrará una serie de afirmaciones. Marque el nivel de acuerdo o desacuerdo según su experiencia. Se utiliza una escala de 1 a 5 donde:

1 = Totalmente en desacuerdo, 2 = En desacuerdo, 3 = Ni de acuerdo ni en desacuerdo, 4 = De acuerdo, 5 = Totalmente de acuerdo

1. Conozco los principios generales de la norma ISO/IEC 27001. *

1 2 3 4 5

2. Tengo noción de los derechos que establece la Ley Orgánica de Protección de Datos Personales (LOPDP). *

1 2 3 4 5

3. En la empresa existen políticas claras sobre el manejo de información confidencial. *

1 2 3 4 5

4. Se aplican buenas prácticas para el manejo de contraseñas y accesos. *

1 2 3 4 5

5. He recibido capacitación sobre seguridad de la información o protección de datos. *

1 2 3 4 5

6. Considero que los sistemas de respaldo de información están correctamente implementados. *

1 2 3 4 5

7. El acceso a los sistemas de la empresa está adecuadamente controlado. *

1 2 3 4 5

8. Uso buenas prácticas al manejar información sensible (clientes, finanzas, etc.). *

FORMATO DE ENCUESTA PREGUNTAS

ANEXO 3

Entrevista Administrativa – Seguridad de la Información en Corbantrade S.A.S.

Estimada Msc. Gallo.

Este formulario es parte de una entrevista administrativa para el proyecto de titulación "Guía para la implementación de políticas de seguridad de la información según la norma ISO/IEC 27001, alineada a la Ley Orgánica de Protección de Datos Personales en Corbantrade S.A.S.".

Le solicitamos que responda con base en su conocimiento sobre el funcionamiento interno de la empresa. Las respuestas serán confidenciales y utilizadas únicamente con fines académicos.

Gracias por su colaboración y tiempo.

1. ¿La empresa cuenta con políticas claras para el manejo de datos de clientes? *

Texto de respuesta larga

2. ¿Ha recibido alguna capacitación sobre protección de datos personales o seguridad informática? *

Texto de respuesta larga

3. ¿Cómo se protegen los documentos o archivos sensibles dentro del área administrativa? *

Texto de respuesta larga

4. ¿Existen procedimientos en caso de incidentes de seguridad digital? *

Texto de respuesta larga

5. ¿Qué tan prioritario cree usted que es implementar políticas de seguridad de la información? *

Texto de respuesta larga

6. ¿Considera útil una guía estructurada basada en normas como la ISO/IEC 27001 y la LOPDP? *

FORMATO DE ENTREVISTA ADMINISTRACIÓN

ANEXO 4

Entrevista Técnica – Seguridad de la Información en Corbantrade S.A.S.

Estimado Ing. Torres.

Este formulario es parte de una entrevista técnica para el proyecto de titulación "Guía para la implementación de políticas de seguridad de la información según la norma ISO/IEC 27001, alineada a la Ley Orgánica de Protección de Datos Personales en Corbantrade S.A.S.".

Le pedimos que responda con base en su experiencia en el área de sistemas. Sus respuestas serán confidenciales y se usarán únicamente con fines académicos.

Agradezco de antemano su tiempo y claridad en las respuestas.

1. ¿Qué controles de seguridad están actualmente implementados en la red y los servidores? *

Texto de respuesta larga

2. ¿Existen políticas formales para la gestión de accesos y contraseñas? *

Texto de respuesta larga

3. ¿Cómo se realiza el respaldo de la información crítica? *

Texto de respuesta larga

4. ¿Se ha presentado algún incidente de seguridad en los últimos años? ¿Cómo fue gestionado? *

Texto de respuesta larga

5. ¿Qué desafíos enfrenta el área de TI en términos de seguridad informática? *

Texto de respuesta larga

6. ¿Considera necesaria una guía para implementar buenas prácticas de seguridad en la empresa? *

FORMATO DE ENTREVISTA SISTEMAS

ANEXO 5

SOCIALIZACÓN AL PERSONAL

ANEXO 6

RIESGOS IDENTIFICADOS

ANEXO 7

MODELO DE IMPLEMENTACIÓN

GLOSARIO

Activo de información

Recurso que contiene datos valiosos para la organización, como bases de datos, servidores, documentos digitales o físicos, cuya protección es fundamental para garantizar la continuidad del negocio.

Amenaza

Evento o circunstancia que puede causar un daño a la información o a los sistemas de la organización, ya sea de origen interno o externo (ejemplo: malware, errores humanos, desastres naturales).

Confidencialidad

Principio de seguridad de la información que garantiza que solo las personas autorizadas puedan acceder a determinados datos.

Disponibilidad

Principio que asegura que la información esté accesible y utilizable por las personas autorizadas siempre que sea necesario.

Firewall

Herramienta de hardware o software que controla el tráfico de red, permitiendo o bloqueando conexiones de acuerdo con políticas de seguridad definidas.

Gestión de riesgos

Proceso mediante el cual se identifican, analizan y tratan los riesgos que pueden afectar a la seguridad de la información.

Integridad

Principio de seguridad que asegura que la información se mantenga exacta, completa y sin alteraciones no autorizadas.

ISO/IEC 27001:2022

Norma internacional que establece los requisitos para implementar, mantener y mejorar un Sistema de Gestión de Seguridad de la Información (SGSI).

LOPDP

Ley Orgánica de Protección de Datos Personales vigente en Ecuador desde 2021, que regula el tratamiento de los datos personales y protege los derechos de los titulares.

Phishing

Técnica de ataque cibernético en la que un atacante suplanta la identidad de una entidad confiable para obtener información confidencial, como contraseñas o datos financieros.

Política de seguridad de la información

Documento oficial de la organización que establece los lineamientos, roles y controles necesarios para proteger los activos de información.

SGSI (Sistema de Gestión de Seguridad de la Información)

Conjunto de políticas, procedimientos, recursos y controles que permiten gestionar de manera estructurada la seguridad de la información dentro de una organización.

Vulnerabilidad

Debilidad en un sistema, proceso o control que puede ser explotada por una amenaza para afectar la seguridad de la información.

ÍNDICE DE FIGURAS Y TABLAS

Figuras

Tablas