UNIVERSIDAD LAICA "ELOY ALFARO" DE MANABÍ

EXTENSIÓN EN EL CARMEN

CARRERA AUDITORÍA Y CONTROL DE GESTIÓN

PROYECTO DE INVESTIGACIÓN

Auditoría informática para salvaguardar los datos en el Centro de Apoyo La U asesora.ec

AUTOR(A):

Michael Rodrigo Morocho Ribadeneira

TUTOR:

Ing. Milton Geovanny Zambrano.

El Carmen, 25 de junio de 2026

CERTIFICACIÓN

En calidad de docente tutor de la Extensión El Carmen de la Universidad Laica "Eloy Alfaro" de Manabí, CERTIFICO:

Haber dirigido, revisado y aprobado preliminarmente el Trabajo de Integración Curricular bajo la autoría del estudiante Michael Rodrigo Morocho Ribadeneira, legalmente matriculada en la carrera de Auditoría y Control de Gestión, período académico 2025-2026, cumpliendo el total de 240 horas, cuyo tema del proyecto o núcleo problémico es "Auditoría informática para salvaguardar los datos en el Centro de Apoyo La U asesora.ec ".

La presente investigación ha sido desarrollada en apego al cumplimiento de los requisitos académicos exigidos por el Reglamento de Régimen Académico y en concordancia con los lineamientos internos de la opción de titulación en mención, reuniendo y cumpliendo con los méritos académicos, científicos y formales, y la originalidad del mismo, requisitos suficientes para ser sometida a la evaluación del tribunal de titulación que designe la autoridad competente.

Particular que certifico para los fines consiguientes, salvo disposición de ley en contrario.

El Carmen, 30 de julio de 2026.

Lo certifico,

Ing. Milton Geovanny Zambrano Rivera, Mgtr.
Docente Tutor
Área: Auditoría, Gestión Contable y Financiera

UNIVERSIDAD LAICA "ELOY ALFARO" DE MANABÍ

EXTENSIÓN EL CARMEN

APROBACIÓN DEL TRABAJO DE TITULACIÓN

Los miembros del Tribunal Examinador aprueban el Trabajo de Titulación con modalidad Proyecto Integrador, titulado "Auditoría informática para salvaguardar los datos en el Centro de apoyo la U Asesor@.ec", cuyo autor es Michael Rodrigo Morocho Ribadeneira, de la Carrera de Auditoría y control de gestión, y como Tutor de Trabajo de Titulación el Ing. Milton Geovanny Zambrano Rivera, Mgtr.

.

El Carmen, 28 de agosto de 2026

Ing. Martha Margarita Minaya Macías, Mgtr.
Presidente del tribunal de titulación

Dra. Nelly Yolanda Moreira Mero, PHD
Miembro del tribunal de titulación

Lcdo. Richard Fernando Hurtado Guevera, Mgtr
Miembro del tribunal de titulación

Uleam

Extensión El Carmen

DECLARACIÓN DE AUTORIA

La responsabilidad de este proyecto de Titulación: "Auditoría informática para salvaguardar los datos en el Centro de Apoyo la U Asesor@.ec", corresponde exclusivamente a Michael Rodrigo Morocho Ribadeneira con C.I 1725402323 y los derechos patrimoniales del mismo a la Universidad Laica Eloy Alfaro de Manabí.

El Carmen – Manabí

Autor

Michael Rodrigo Morocho Ribadeneira
C.I 1725402323

DEDICATORIA

A Dios, por guiar cada uno de mis pasos, concederme sabiduría, fortaleza y perseverancia para superar los desafíos de este camino y permitirme alcanzar esta meta.

A mi padre, Tirso Rodrigo Morocho Huilca, a quien dedico este trabajo con todo mi corazón. Gracias por creer en mí incluso cuando yo mismo dudaba de mis capacidades, por nunca abandonarme y por brindarme siempre tu apoyo incondicional. Tu ejemplo de esfuerzo, honestidad y perseverancia ha sido la inspiración que me impulsó a seguir adelante. Este logro también es tuyo, porque sin ti no habría sido posible alcanzar este sueño.

A la familia Hernández, por su apoyo, confianza y generosidad durante este proceso. Su compañía y sus palabras de aliento fueron una motivación constante para continuar hasta el final de esta etapa.

Finalmente, dedico este trabajo a todas las personas que, de una u otra manera, estuvieron presentes a lo largo de este camino, brindándome su apoyo y motivación para no rendirme.

AGRADECIMIENTO

Expreso mi más sincero agradecimiento a Dios, por permitirme culminar esta importante etapa de mi vida y por concederme la fortaleza, la sabiduría y la perseverancia necesarias para alcanzar esta meta.

A mi padre, Tirso Rodrigo Morocho Huilca, por su esfuerzo, confianza y apoyo incondicional a lo largo de mi formación. Gracias por hacer posible que este sueño hoy sea una realidad.

A la familia Hernández, por su generosidad, confianza y respaldo durante este camino. Su apoyo fue fundamental para continuar con determinación hasta alcanzar este objetivo.

A una persona muy especial, cuyo apoyo, comprensión y compañía representaron un valioso sostén en los momentos más desafiantes. Gracias por brindarme tranquilidad cuando más la necesité y por motivarme a seguir adelante. Tu presencia dejó una huella significativa en este logro.

A la Universidad Laica Eloy Alfaro de Manabí, a los docentes de la carrera de Auditoría y Control de Gestión y a mi tutor de trabajo de titulación, por los conocimientos, orientaciones y aportes brindados durante el desarrollo de esta investigación.

Finalmente, expreso mi gratitud a todas las personas que, de una u otra manera, contribuyeron al cumplimiento de este objetivo académico.

ÍNDICE GENERAL

RESUMEN

El presente proyecto de investigación analizó la auditoría informática y su relación con la salvaguarda de los datos en el Centro de Apoyo La U asesora.ec, con el objetivo de diseñar un modelo de auditoría informática basado en ISO/IEC 27001:2022 para fortalecer la protección de la información. Se empleó un enfoque mixto cualitativo-cuantitativo, con diseño no experimental, transversal y alcance descriptivo. La encuesta se aplicó de forma censal al 100 % de la población definida, conformada por 40 participantes: 36 estudiantes de vinculación y 4 docentes supervisores; adicionalmente, la persona responsable del Centro participó como informante clave mediante una entrevista semiestructurada. La información se complementó con análisis documental, observación directa y una lista de verificación. Los resultados evidenciaron debilidades relacionadas con la formalización de políticas, gestión de accesos, respaldos, riesgos y seguimiento de controles. A partir del diagnóstico se estructuró una guía de seguridad de la información que integra lineamientos, responsabilidades, procedimientos y formatos orientados a organizar estas prácticas y fortalecer progresivamente la salvaguarda de los datos del Centro.

Palabras clave: auditoría informática, seguridad de la información, salvaguarda de datos, controles de TI, gestión de riesgos.

INTRODUCCIÓN

El avance de las tecnologías de la información ha incrementado la cantidad de datos que las organizaciones generan, procesan y almacenan durante sus actividades, lo que también exige mayores medidas para protegerlos. En este contexto, la auditoría informática constituye un mecanismo de evaluación que permite examinar recursos tecnológicos, controles y evidencias con el propósito de identificar condiciones que puedan afectar la confidencialidad, integridad y disponibilidad de la información. La incorporación de estándares y buenas prácticas contribuye a orientar estas evaluaciones y a establecer criterios acordes con los riesgos presentes en cada organización (Whitman & Mattord, 2022; ISO, 2022c).

En Ecuador, la protección de la información adquiere además una dimensión jurídica a partir de la Ley Orgánica de Protección de Datos Personales, que establece obligaciones relacionadas con la seguridad de los datos y la adopción de medidas apropiadas frente a los riesgos derivados de su tratamiento (Asamblea Nacional del Ecuador, 2021). En el ámbito técnico, ISO/IEC 27001:2022 proporciona requisitos para la gestión de la seguridad de la información, mientras que ISO/IEC 27002:2022 orienta la aplicación de controles relacionados con aspectos organizacionales, humanos, físicos y tecnológicos (ISO, 2022b, 2022c). Estos referentes permiten vincular las obligaciones de protección con mecanismos que puedan ser examinados mediante evidencias y registros.

En el ámbito específico del Centro de Apoyo La U asesora.ec, las actividades de vinculación desarrolladas por docentes y estudiantes requieren el uso de recursos tecnológicos y el manejo de información académica, administrativa y relacionada con los beneficiarios. Esta dinámica genera necesidades asociadas con el control de accesos, la asignación de responsabilidades, los respaldos, la recuperación de información y la gestión de riesgos. Ante estas condiciones, la investigación se orientó a examinar la situación de los controles

relacionados con la salvaguarda de los datos y a establecer alternativas que contribuyan a su fortalecimiento.

La importancia del estudio radica en disponer de información sustentada sobre las condiciones en que se gestionan los datos dentro del Centro, diferenciando las prácticas declaradas de aquellas que pueden comprobarse mediante documentación y otros registros. En correspondencia con esta necesidad, el objetivo general se orientó a diseñar un modelo de auditoría informática basado en ISO/IEC 27001:2022 para fortalecer la salvaguarda de los datos en el Centro de Apoyo La U asesora.ec. Para su cumplimiento se abordaron como variables la auditoría informática y la salvaguarda de los datos, estableciendo una relación entre la evaluación de los controles tecnológicos y las medidas destinadas a proteger la información.

El desarrollo de la investigación comprendió el análisis histórico del objeto y campo de estudio, la fundamentación teórica de las variables, el diagnóstico de la situación actual y la elaboración de una propuesta derivada de las necesidades identificadas. Se adoptó un enfoque mixto cualitativo-cuantitativo, con predominio cuantitativo, diseño no experimental, transversal y alcance descriptivo. Se emplearon los métodos inductivo, deductivo, histórico-lógico, bibliográfico y analítico-sintético, mientras que para la recolección y contraste de información se utilizaron la encuesta, la entrevista semiestructurada, el análisis documental, la observación directa y una lista de verificación.

En el componente cuantitativo se aplicó la encuesta de manera censal al 100 % de la población definida, constituida por 40 participantes: 36 estudiantes de vinculación y 4 docentes supervisores. De forma independiente, la persona responsable del Centro participó como informante clave mediante una entrevista semiestructurada y no fue incluida dentro de los 40 participantes de la encuesta. La información recopilada mediante los diferentes instrumentos fue contrastada para distinguir las percepciones de los participantes de la evidencia disponible sobre los controles examinados. Esta delimitación permitió mantener los resultados

circunscritos al Centro y al periodo analizado, sin pretender generalizarlos a toda la infraestructura tecnológica de la Universidad.

Los resultados mostraron principalmente necesidades de formalización y organización en las prácticas relacionadas con la seguridad de la información. Se identificaron condiciones que requieren atención en las políticas de seguridad, administración de cuentas y permisos, respaldo y recuperación de información, gestión de riesgos y seguimiento de controles. La integración de la encuesta, la entrevista y la evidencia examinada permitió sustentar los hallazgos y establecer los aspectos que debían ser considerados en la propuesta.

A partir de estos resultados se estructuró una guía de seguridad de la información para el Centro de Apoyo La U asesora.ec, conformada por lineamientos, responsabilidades, procedimientos y formatos de apoyo. Su contenido aborda aspectos relacionados con la gestión de accesos, respaldo y recuperación, valoración y tratamiento de riesgos, así como la revisión y seguimiento de controles. La propuesta se plantea como una herramienta adaptable a las condiciones del Centro y su aplicación queda sujeta a la revisión y autorización de las instancias institucionales competentes.

El trabajo se encuentra organizado en tres capítulos. El Capítulo I desarrolla la fundamentación teórica relacionada con la auditoría informática y la salvaguarda de los datos; el Capítulo II presenta las características del Centro, la metodología aplicada, la ejecución del diagnóstico y el análisis de los resultados obtenidos; y el Capítulo III desarrolla la propuesta de la guía de seguridad de la información a partir de las necesidades identificadas. Finalmente, se presentan las conclusiones, recomendaciones, referencias bibliográficas y anexos que respaldan el proceso investigativo.

CAPÍTULO I

1. MARCO TEÓRICO

1.1 Fundamentos de la auditoría informática

Burgos-Rojas et al. (2024) destacan la utilidad de integrar marcos de seguridad en las auditorías informáticas, ya que proporcionan criterios para estructurar y sustentar la evaluación. La auditoría informática se aborda como un proceso de evaluación que permite examinar los recursos tecnológicos, los sistemas de información y los controles establecidos, y determinar qué riesgos afectan a la información, qué controles existen para enfrentarlos y qué evidencia demuestra su funcionamiento.

Para Slapničar et al. (2022), la efectividad de la auditoría de ciberseguridad se relaciona con la madurez alcanzada en la gestión de riesgos, por lo que, a partir de la evidencia disponible, se puede establecer qué controles funcionan, cuáles presentan debilidades y dónde se requiere intervenir. Por lo tanto, una auditoría no solo se evalúa por los buenos resultados con una lista de verificación; es mejor realizarla con el alcance de la auditoría, la competencia del auditor y la calidad de la evidencia como criterios, y sacar conclusiones.

Sabillon et al. (2024) indican que, para organizar la evaluación, hay cuatro referencias y cada una tiene una importancia distinta: ISO/IEC 27001:2022 para propósitos de seguridad; ISO 19011:2026 para el proceso de auditoría; COBIT para gobernanza y gestión; y el Marco de Ciberseguridad 2.0 del Instituto Nacional de Estándares y Tecnología (NIST). Organiza los resultados de ciberseguridad (ISO, 2022a, 2026; NIST, 2024). La utilización conjunta exige evitar duplicidades y mantener la trazabilidad entre riesgo, control, prueba y evidencia

(Antunes et al., 2022; Burgos-Rojas et al., 2024). Para Taherdoost (2022), la selección debe responder al propósito, al tamaño y a los recursos disponibles de la organización.

En Ecuador, la auditoría informática también permite verificar el cumplimiento de las obligaciones relativas al tratamiento de datos personales. En este sentido, Lucero (2023) explica que estas obligaciones deben traducirse en controles verificables en los sistemas y procesos institucionales, ya que se manejan registros académicos y administrativos cuya protección requiere responsabilidades definidas, así como procesos y mecanismos de seguimiento.

1.1.1 Auditoría informática y control interno

El marco COSO para el control interno organiza la manera en que una entidad administra sus riesgos y procura una seguridad razonable respecto de sus objetivos operativos, de información y de cumplimiento (Littan et al., 2023) indica que este sistema se estructura en cinco componentes interrelacionados:

1) ambiente de control.
2) Evaluación de riesgos
3) Actividades de control
4) Información y comunicación.
5) Actividades de monitoreo.

En el ámbito tecnológico, estos componentes ofrecen una base para revisar responsabilidades, la administración de usuarios, la segregación de funciones, los accesos, los respaldos, la protección de bases de datos y el seguimiento de incidentes, profundizando en el trabajo de auditoría, ya que se valida si los controles se aplican de forma consistente y producen el resultado previsto (Littan et al., 2023). La integración de los controles con los procesos y responsabilidades institucionales facilita su seguimiento, mientras que los hallazgos

respaldados por evidencia orientan las decisiones y las acciones correctivas (Antunes et al., 2022 ; Slapničar et al., 2022).

Desde enfoques diferentes, COBIT e ISO/IEC 27001:2022 aportan a la evaluación de la seguridad de la información. COBIT ayuda a relacionar la gestión tecnológica con las prioridades de la institución, los riesgos existentes y la distribución de responsabilidades, tomando en cuenta su tamaño y capacidad operativa. En cambio, ISO/IEC 27001:2022 orienta la identificación de los riesgos de seguridad, la selección de controles adecuados y la evaluación del desempeño del sistema de gestión (Rafeq & Elangovan, 2021; ISO, 2022a).

1.1.2 Seguridad de la información

La gestión de la seguridad se comprende mejor cuando se analiza en situaciones reales, porque integra no solo la tecnología, sino también a las personas, los procedimientos y la supervisión, como señalan Whitman y Mattord (2022).

Un sistema de gestión de la seguridad de la información (SGSI) organiza las decisiones en función del contexto institucional. Este proceso comprende las responsabilidades, la valoración de riesgos, el tratamiento y la revisión del desempeño (AlGhamdi et al., 2020; ISO, 2022c). La norma ISO/IEC 27001:2022 establece los requisitos del sistema; la literatura sobre su adopción muestra que el apoyo directivo, la asignación de funciones, así como el comportamiento de los usuarios influyen en su funcionamiento (AlGhamdi et al., 2020; ISO, 2022c).

En Ecuador, la seguridad de la información también forma parte de la Estrategia Nacional de Ciberseguridad (Ministerio de Telecomunicaciones y de la Sociedad de la Información, 2022). En cuanto a la protección de datos personales, la LOPDP establece obligaciones relacionadas con la seguridad y la responsabilidad demostrada (Asamblea Nacional del Ecuador, 2021), que se complementan con el Reglamento General de la Ley Orgánica de Protección de Datos Personales (Presidencia de la República del Ecuador, 2023).

Para organizar el análisis de la ciberseguridad, el NIST (2024) plantea seis funciones dentro del Marco de Ciberseguridad 2.0: Govern, Identify, Protect, Detect, Respond y Recover. De forma complementaria, Joint Task Force (2020) señala en NIST SP 800-53 Rev. 5 que los controles no deben aplicarse como una lista obligatoria para todos los casos, sino que pueden seleccionarse según las características y necesidades de cada entorno. Esta selección resulta especialmente importante en organizaciones con recursos limitados, ya que permite priorizar los riesgos más relevantes antes de atender otros aspectos de menor impacto (Chidukwani et al., 2022).

Desde la perspectiva de auditoría, Schmitz et al. (2021) indican que la aplicación debe comprobarse mediante registros, configuraciones y evidencias que permitan conocer lo que realmente ocurre durante las actividades habituales, ya que la valoración considera tanto la implementación del control como la evidencia disponible para sustentarla (Schmitz et al., 2021).

1.1.3 Norma ISO/IEC 27001:2022

La ISO/IEC 27001:2022 sirve de referencia para organizar la gestión de la seguridad de la información de acuerdo con las características y los riesgos de cada organización. Para ello, aborda aspectos relacionados con el contexto institucional, el liderazgo, la planificación, el apoyo, la operación, la evaluación del desempeño y la mejora. La norma también incorpora en su Anexo A un conjunto de controles que pueden considerarse al abordar los riesgos identificados. Esto no supone aplicar todos los controles de manera indistinta, pues su selección requiere una justificación acorde con las necesidades de la organización (ISO, 2022c).

Al examinar un riesgo, es necesario partir del activo o del proceso involucrado y determinar qué situaciones podrían afectarlo. La ISO/IEC 27005:2022 orienta este trabajo mediante la identificación, el análisis, la evaluación y el tratamiento de los riesgos (ISO, 2022a). En la presente investigación, este proceso permite relacionar cada escenario

identificado con el control correspondiente a revisar, la evidencia necesaria para comprobarlo y el resultado obtenido durante la evaluación. Mantener esta relación facilita el seguimiento de lo realizado y evita incorporar controles sin una razón sustentada en el riesgo analizado (Sánchez-García et al., 2023).

La planificación, la operación, la evaluación del desempeño y la mejora forman parte de la gestión establecida por la norma y responden también a la lógica del ciclo PHVA. Sin embargo, en el Centro, considerar estas etapas no es suficiente para afirmar que el ciclo se cumple. La revisión permite comprobar quién asume cada responsabilidad, qué actividades se registran y qué seguimiento se ha realizado (ISO, 2022c). Esta verificación ayuda a distinguir entre un control que únicamente consta en los documentos y otro cuya aplicación puede comprobarse mediante registros y resultados.

Los controles del Anexo A están agrupados en cuatro ámbitos: a) organizacionales, b) personas, c) físicos y d) tecnológicos. La ISO/IEC 27002:2022 complementa esta estructura con directrices para su aplicación (ISO, 2022b). COBIT 2019 se reserva para examinar responsabilidades y gobernanza, mientras que NIST CSF 2.0 permite organizar los resultados de ciberseguridad (NIST, 2024; Rafeq & Elangovan, 2021).

Las experiencias estudiadas en instituciones de educación superior, como las de Cheng y Wang (2022), permiten reconocer problemas asociados con los usuarios, los servicios digitales y la diversidad de recursos tecnológicos existentes. Por su parte, Ulven y Wangen (2021) indican que, en las organizaciones de menor escala, resulta conveniente atender primero los controles vinculados con las necesidades de mayor prioridad.

1.1.4 COBIT 2019 y otros marcos internacionales de referencia

COBIT 2019 permite examinar el gobierno y la gestión de la información y la tecnología considerando las necesidades de las partes interesadas, los riesgos y los recursos disponibles. Dentro de este marco, el gobierno se ocupa de evaluar las necesidades, orientar las

decisiones y supervisar sus resultados, mientras que la gestión comprende la planificación, construcción, ejecución y monitoreo de las actividades. Esta diferencia resulta útil en el Centro porque permite reconocer quién autoriza un control, quién se encarga de aplicarlo y quién verifica su cumplimiento, evitando que todas estas responsabilidades recaigan sobre una misma función sin la debida supervisión (Rafeq & Elangovan, 2021).

Pawar & Palivela (2022) indican que COBIT organiza los objetivos en los dominios EDM, APO, BAI, DSS y MEA. Sin embargo, la investigación no requiere abordar todos ellos, ya que el interés se centra en los aspectos relacionados con los riesgos, la seguridad, la continuidad, las operaciones y el seguimiento. En consecuencia, su incorporación al estudio no constituye una evaluación completa de la madurez de COBIT. El marco se emplea específicamente para analizar la asignación de responsabilidades, la alineación institucional y la supervisión de los controles considerados durante la auditoría (Rafeq & Elangovan, 2021).

1.2 Salvaguarda de los datos

1.2.1 Conceptualización de la salvaguarda de los datos

La protección de la información durante su uso, almacenamiento, transmisión, conservación y eliminación requiere medidas organizativas y técnicas que permitan mantener la confidencialidad, la integridad, la disponibilidad y la capacidad de recuperación de los datos. En la práctica, estas medidas se reflejan en políticas, responsabilidades y controles preventivos, de detección y correctivos, los cuales deben seleccionarse de acuerdo con las necesidades y los riesgos identificados (ISO, 2022b).

Desde un enfoque orientado a resultados, el NIST (2020) señala que la protección de la información debe considerar los riesgos relacionados con la pérdida, alteración o falta de disponibilidad de los datos. Bajo esta perspectiva, la privacidad resulta importante cuando el tratamiento de la información puede generar consecuencias para sus titulares.

En Ecuador, la LOPDP recoge los principios de juridicidad, transparencia, finalidad, pertinencia, minimización, seguridad y responsabilidad proactiva y demostrada (Asamblea Nacional del Ecuador, 2021). La Estrategia Nacional de Ciberseguridad incorpora aspectos relacionados con la resiliencia y el fortalecimiento de las capacidades institucionales (Ministerio de Telecomunicaciones y de la Sociedad de la Información, 2022).

Sabillon et al. (2024) muestran que los modelos de auditoría de ciberseguridad pueden organizarse en dominios, criterios, subcriterios y pruebas, vinculando el riesgo identificado con el criterio de revisión, el procedimiento aplicado, la evidencia obtenida y el hallazgo resultante.

1.2.2 Importancia de la salvaguarda de los datos

Whitman & Mattord (2022) refieren que una pérdida, alteración o indisponibilidad puede afectar las actividades, además de producir consecuencias jurídicas y reputacionales, constituyendo la protección de datos como una responsabilidad institucional compartida. La ISO/IEC 27005:2022 orienta la identificación, el análisis, la evaluación y el tratamiento de los riesgos de seguridad de la información (ISO, 2022a). La relación documentada entre cada escenario y su contramedida ayuda a justificar las decisiones y a concentrar los recursos en los riesgos de mayor relevancia (Sánchez-García et al., 2023).

Prümmer et al. (2024) sostienen que la formación en ciberseguridad debe considerar tanto el comportamiento como el contexto de los usuarios. También Shillair et al. (2022) incluyen la educación, la sensibilización y la capacitación entre las capacidades necesarias para mantener la ciberseguridad.

La LOPDP (2021) indica que el tratamiento debe responder a la finalidad para la cual se recopilaron los datos y, además, el responsable debe estar en condiciones de demostrar las medidas adoptadas para su protección (Asamblea Nacional del Ecuador, 2021). En este sentido, Garcés et al. (2023) indican que mantener o eliminar estos archivos es un proceso que siempre

dependerá del propósito original de los datos, de las leyes vigentes en ese momento y de los derechos de las personas implicadas.

Slapničar et al. (2022) relacionaron la calidad de la planificación, la ejecución y el informe de la auditoría con la madurez de la gestión del riesgo; esta relación no implica que la auditoría elimine la posibilidad de incidentes, por lo que la auditoría es relevante porque aporta evidencia para distinguir entre controles documentados y controles que funcionan en la práctica.

1.2.3 Ley Orgánica de Protección de Datos Personales (LOPDP)

La Ley Orgánica de Protección de Datos Personales regula el tratamiento de información que identifica a una persona natural, el alcance sobre la seguridad de archivos digitales, reconoce derechos de los titulares y establece obligaciones para quienes deciden las finalidades y los medios del tratamiento, así como para quienes procesan los datos por cuenta de estos (Asamblea Nacional del Ecuador, 2021).

En materia de seguridad, la LOPDP dispone que las medidas deben responder a la naturaleza, el volumen y los riesgos del tratamiento, exigiendo examinar la confidencialidad, la integridad, la disponibilidad y la capacidad de recuperación de los datos, además de verificar periódicamente la eficacia de los controles adoptados (Asamblea Nacional del Ecuador, 2021, art. 37).

El Reglamento General de la Ley de Protección de Datos Personales indica que, dentro de la lógica de una auditoría, estas reglas necesitan materializarse en evidencias verificables. Esto supone contar con tiempos de conservación definidos, inventarios, políticas aprobadas y directrices para responder ante incidentes, procurando además que pueda identificarse al responsable de cada actividad.

1.2.4 Principios de protección de datos

El artículo 10 de la LOPDP reconoce los principios de juridicidad, lealtad, transparencia, finalidad, pertinencia y minimización, así como la responsabilidad proactiva y

demostrada de la aplicación favorable al titular, donde la coincidencia textual en sus nombres es necesaria, debido a que se trata de denominaciones legales que no deben alterarse mediante sinónimos (Asamblea Nacional del Ecuador, 2021, art. 10).

El reglamento general de la ley establece responsabilidades asignadas, políticas aprobadas, autorizaciones de acceso, registros de incidentes, pruebas de restauración y evidencias de las capacitaciones realizadas; también complementa este principio al desarrollar procedimientos para la aplicación de las obligaciones legales a fin de contrastar con la documentación disponible y con las prácticas que puedan comprobarse durante la revisión (Presidencia de la República del Ecuador, 2023).

ISO/IEC 27001:2022 proporciona requisitos para la gestión de la seguridad de la información, mientras que ISO/IEC 27002:2022 aporta orientaciones para la aplicación de los controles de seguridad (ISO, 2022b, 2022c). A estos referentes se incorpora el NIST Privacy Framework, utilizado para organizar el análisis de los riesgos que el tratamiento puede generar para los titulares de los datos (NIST, 2020). En este sentido, facilitan los estándares técnicos para la evaluación, facilitando las obligaciones establecidas en la LOPDP.

CAPÍTULO II

2. DIAGNÓSTICO O ESTUDIO DE CAMPO

Este capítulo presenta el diagnóstico del Centro de Apoyo La U asesora.ec. El estudio se desarrolló con un enfoque mixto cualitativo-cuantitativo, diseño no experimental, corte transversal y alcance descriptivo. La integración de encuesta, entrevista y evidencia documental permitió contrastar percepciones con prácticas observables y registros disponibles, conforme a la lógica de los diseños mixtos (Creswell & Creswell, 2022; Saunders et al., 2023).

La encuesta se aplicó de forma censal a 41 participantes: 36 estudiantes de vinculación, 4 docentes supervisores y el responsable del Centro. La unidad de análisis del checklist fue la organización y sus controles; su aplicación incluyó revisión documental y observación directa.

2.1 Naturaleza de la empresa

El Centro de Apoyo La U asesora.ec es un proyecto de vinculación de la Universidad Laica Eloy Alfaro de Manabí, en la extensión El Carmen. Su naturaleza es académica y social, ya que involucra a profesores (y estudiantes) que trabajan conjuntamente con otros para proporcionar asesoría y apoyo gratuitos en gestión empresarial y emprendimiento a los beneficiarios de su área (ULEAM, 2025).

El proyecto desarrolla procesos de diagnóstico, capacitación, asistencia técnica, monitoreo y evaluación (ULEAM, 2025), y durante estos procesos se proporciona información académica, administrativa, técnica y personal a los usuarios. Por lo tanto, para registrar, consultar, comunicar y conservar esa información se emplean equipos informáticos, aplicaciones de oficina, medios de comunicación digitales y espacios de almacenamiento electrónico. Ya que la intervención de diferentes actores y el uso compartido de recursos

tecnológicos generan necesidades concretas de control de cuentas, permisos, custodia documental, respaldos y disponibilidad de la información.

Por esta razón, el alcance de la investigación se limita a los datos, recursos y controles empleados en las actividades del Centro. El diagnóstico detalla su condición durante el período analizado y aporta evidencia para la propuesta, sin extrapolar los resultados a toda la infraestructura tecnológica de la Universidad.

2.2 Descripción del Centro de Apoyo La U Asesor@.ec

La documentación institucional presenta la iniciativa como un Centro de Apoyo y Asesoría Gratuita en la Gestión Empresarial y de Emprendimiento, La U Asesora.ec. Este proyecto forma parte de las actividades de vinculación de la Universidad Laica Eloy Alfaro de Manabí, en su extensión El Carmen. Para mantener la correspondencia con el título aprobado de la investigación, en el resto del documento se emplea la denominación abreviada Centro de Apoyo La U asesora.ec.

Según la documentación examinada durante el trabajo de campo, el proyecto fue aprobado mediante la Resolución del Consejo de Extensión N.° CE-SO-04-No.06-2025 y su periodo de ejecución comprende desde abril de 2025 hasta enero de 2029. En su desarrollo participan las carreras de Administración, Agronegocios, Finanzas y Auditoría y Control de Gestión, bajo la coordinación del Ing. Milton G. Zambrano Rivera, Mg. Estos datos corresponden al periodo considerado en la investigación y deben respaldarse con la guía institucional o con el documento incorporado en los anexos.

Las actividades del Centro incluyen diagnóstico, capacitación, asistencia técnica, seguimiento y evaluación de los servicios ofrecidos a emprendedores y organizaciones, en los que intervienen docentes y estudiantes, quienes producen y consultan información académica, administrativa y técnica relacionada con los beneficiarios.

Se emplean recursos técnicos y tecnológicos para registrar, procesar, consultar y preservar la información generada durante la asesoría y el seguimiento. Para los propósitos de esta auditoría, la unidad es el conjunto de procesos, registros, recursos y controles relacionados con el Centro; los hallazgos se interpretan como una revisión general de los sistemas de la Universidad Laica Eloy Alfaro de Manabí.

Figura 1. Logotipo del proyecto La U Asesor@.ec

Nota. Extraído de la guía del Proyecto de Vinculación y Emprendimiento de la Universidad Laica Eloy Alfaro de Manabí, Extensión El Carmen (2025).

El logotipo actúa como identificador visual del proyecto en sus documentos y canales de comunicación. Identifica al Centro, pero no significa aprobación de procesos o asignación de deberes, ni cumplimiento de medidas de control.

Eslogan

“Innovando por Ti”.

El eslogan forma parte de la identidad comunicativa del Centro y refleja una orientación hacia la innovación en la atención a los beneficiarios. Sin embargo, esta declaración no señala un proceso formalizado de innovación ni de mejora continua.

2.3 Aspectos de mercado

Debido al carácter gratuito de los servicios del centro coma el análisis de mercado se orienta a identificar la población beneficiaria coma su cobertura y las principales necesidades atendidas coma en lugar de analizar una dinámica comercial punto el proyecto está dirigido a personas naturales y unidades del sector de la economía social, con estimado de 2171

beneficiarios directos punto según la documentación institucional revisada su cobertura comprende Manabí y Santo Domingo de los Tsáchilas, con mayor atención en los cantones el Carmen y Santo Domingo y sus zonas de influencia.

Las necesidades atendidas se relacionan principalmente con la gestión empresarial coma el acceso financiamiento y la formalización de los emprendimientos. También se consideran requerimientos de asesoría en emprendimiento, contabilidad y tributación, finanzas, presupuestos y proyectos de inversión. Frente a estas necesidades, el centro desarrolla actividades de capacitación, asesoría y acompañamiento técnico dirigido Asus beneficiarios.

2.4 Aspecto técnico

Durante el trabajo de campo se observó que el centro utilizo equipos informáticos, aplicaciones de oficina, servicios de comunicación y medios de almacenamiento electrónico para desarrollar sus actividades. Desde el aspecto técnico, la revisión se concentró en las condiciones relacionadas con el acceso de la información, autenticación, permisos, respaldo y recuperación, así como en los registros disponibles para verificar estas actividades.

Los recursos son utilizados por docentes, supervisores y estudiantes de las carreras de Administración, Agronegocios, Finanzas y Auditoría y Control de Gestión. Las actividades involucradas requieren la gestión de la información académica y administrativa, así como la de los usuarios. Por esta razón, los puntos técnicos considerados en el diagnóstico fueron las cuentas y los permisos a los que tenían acceso, el almacenamiento de registros, la ejecución de copias de seguridad y la disponibilidad de la información.

La evaluación comparó las prácticas declaradas con la documentación, la observación y la lista de verificación, y diferencia los controles existentes, los informales y aquellos sin evidencia. La presencia de equipos o aplicaciones no garantizaba la protección. Debido a que este es un estudio descriptivo, no incluyó pruebas de penetración, análisis forense, explotación

de vulnerabilidades ni cambios en el sistema. Los resultados se basan en los controles administrativos y tecnológicos aplicados a las actividades del Centro y no constituyen una evaluación completa de toda la infraestructura de TI de la Universidad.

2.5 Marco estratégico del Centro de Apoyo.

Durante el diagnóstico se revisó la documentación disponible con el propósito de identificar los elementos que orientan estratégicamente el funcionamiento del Centro. Al formar parte de un proyecto de vinculación de la ULEAM, sus actividades se desarrollan dentro de los lineamientos institucionales y de las directrices aplicables al proyecto.

En los documentos examinados no se identificaron instrumentos propios del Centro que establecieran de manera específica su misión, visión, principios y valores. Esta situación evidencia una necesidad de formalización de su direccionamiento, aunque no constituye por sí misma un incumplimiento relacionado con la seguridad de la información.

A partir de esta situación, en el Capítulo III se proponen misión, visión y valores como elementos complementarios para orientar las responsabilidades y actividades del Centro. Estos componentes no sustituyen los controles relacionados con accesos, respaldos, incidentes, riesgos u otras medidas de seguridad identificadas durante el diagnóstico.

2.6 Metodología

Se utilizó un enfoque mixto cualitativo-cuantitativo, con predominio del cuantitativo, y se adoptó un diseño no experimental, transversal y de alcance descriptivo. La encuesta proporcionó frecuencias y porcentajes sobre las percepciones de los participantes; la entrevista ofreció información cualitativa sobre el contexto y las prácticas reportadas por la persona a cargo del Centro; mientras que el análisis documental, la observación directa y la lista de verificación permitieron examinar la evidencia disponible sobre los controles.

Las fuentes se integraron por convergencia durante la interpretación de los resultados. Para ello, se compararon las respuestas de los participantes, la información obtenida mediante la entrevista y la documentación disponible. El estudio no manipuló variables, no aplicó pruebas inferenciales ni buscó demostrar relaciones causales o generalizar estadísticamente los resultados fuera del grupo estudiado (Creswell & Creswell, 2022; Saunders et al., 2023).

2.6.1 Población y estrategia censal

La población considerada para la encuesta estuvo integrada por 40 personas vinculadas con las actividades del Centro de Apoyo La U asesora.ec: 36 estudiantes de vinculación y 4 docentes supervisores. Su inclusión respondió a la participación que mantenían en procesos relacionados con el uso de recursos tecnológicos o el manejo de información pertinente para el diagnóstico.

Al tener acceso a la totalidad de los integrantes, la encuesta se aplicó mediante una estrategia censal. En consecuencia, no se efectuó una selección probabilística ni se calculó un tamaño de muestra diferente de la población estudiada.

2.6.2 Muestra y unidades de análisis

Debido al carácter censal del estudio, se consideró el 100 % de la población definida para la encuesta, conformada por 40 participantes: 36 estudiantes de vinculación y 4 docentes supervisores. Por esta razón, no se realizó cálculo ni selección de una muestra.

Para el componente cualitativo, participó como informante clave la persona responsable del Centro mediante una entrevista semiestructurada. Este informante no formó parte de los 40 participantes considerados en la encuesta.

2.6.3 Métodos de investigación

2.6.3.1 Método inductivo

Las respuestas de la encuesta y la entrevista se analizaron junto con los resultados de la lista de verificación para identificar patrones recurrentes en los controles de seguridad de la

información del Centro. A partir de estas observaciones particulares se determinaron fortalezas y debilidades que sustentaron el diagnóstico y orientaron la formulación de la propuesta. Este procedimiento corresponde a la lógica inductiva, mediante la cual se construye una interpretación a partir de la evidencia obtenida, sin extender los resultados más allá del caso estudiado (Saunders et al., 2023).

2.6.3.2 Método deductivo

Se utilizó el método deductivo para transferir los criterios generales de auditoría, seguridad de la información y protección de datos al análisis específico del Centro de Apoyo La U Asesor@.ec (Saunders et al., 2023). Con el fin de identificar los aspectos que serían revisados mediante los instrumentos, se utilizaron como puntos de referencia la norma ISO/IEC 27001:2022 y la Ley Orgánica de Protección de Datos Personales. Con base en estos criterios, la evidencia recopilada en el Centro se comparó con las prácticas y controles esperados. Dado que el análisis se limitó a los controles incorporados en el diagnóstico, los resultados no constituyen una certificación de la norma ni una evaluación integral del cumplimiento legal..

2.6.3.3 Método Histórico-Lógico

El método histórico-lógico se aplicó con un alcance documental para organizar los antecedentes examinados en el Capítulo I y reconocer los cambios relevantes en el alcance de la auditoría informática, los estándares de seguridad y el marco ecuatoriano de protección de datos. Esta revisión permitió situar el problema del Centro de Apoyo La U asesora.ec en su contexto técnico y normativo. El procedimiento tuvo una finalidad interpretativa y no incluyó mediciones longitudinales ni una serie temporal de datos empíricos.

2.6.3.4 Método Bibliográfico

Se utilizó el método bibliográfico para establecer las categorías del estudio y los criterios técnicos y legales que orientaron la elaboración de los instrumentos (Creswell & Creswell, 2022; Saunders et al., 2023). Para el diagnóstico y la propuesta se tomaron como

referencias principales la ISO/IEC 27001:2022 y la Ley Orgánica de Protección de Datos Personales. Además, se revisaron artículos científicos, libros especializados, normas técnicas, legislación y documentos oficiales publicados desde 2020.

La selección de las fuentes se realizó considerando su relación con la auditoría de TI, la seguridad de la información, la protección de datos personales, el control interno y los riesgos tecnológicos. También se tomó en cuenta la autoría de cada documento y la posibilidad de comprobar su origen. En contraste, la documentación interna del Centro se utilizó como evidencia del caso y se examinó mediante la revisión documental y el cuestionario de control interno estructurado como lista de verificación.

2.6.3.5 Método Analítico-Sintético

El método analítico-sintético se utilizó en dos fases. En la primera, analizamos cuidadosamente los resultados de encuestas, entrevistas, revisión documental y listas de control, organizándolos claramente según las categorías de control evaluadas. En la segunda fase, combinamos toda esta información para comparar las percepciones de los participantes, las prácticas declaradas y la evidencia recopilada, manteniendo un registro organizado de cada resultado y siguiendo el enfoque de métodos mixtos (Creswell & Creswell, 2022). Este proceso nos permitió organizar los resultados en condiciones, criterios, causas, efectos o riesgos, evidencia y recomendaciones, e identificar los requisitos que debía cumplir el modelo de auditoría de TI.

2.7 Técnicas de investigación

Para el diagnóstico se aplicaron diferentes técnicas, según la información que se necesitaba obtener. Primero, la entrevista permitió conocer las prácticas realizadas por la persona responsable del Centro. Luego, la encuesta recogió las opiniones de los estudiantes y de los docentes supervisores. Además, la revisión de documentos y la observación directa

ayudaron a comprobar la información disponible. Y, por último, el cuestionario de control interno se organizó como una lista de verificación. La información obtenida mediante estas técnicas se contrastó durante la interpretación de los resultados.

2.7.1 Planificación del diagnóstico de los controles

Antes de ejecutar el diagnóstico se realizó una planificación para organizar la revisión de los controles relacionados con la salvaguarda de los datos en el Centro de Apoyo La U Asesor@.ec. En esta etapa se establecieron el motivo de la revisión, el objetivo, el alcance, los aspectos a examinar, las fuentes de información, los procedimientos e instrumentos y la forma en que serían analizados los resultados. Esta organización permitió definir previamente qué se revisaría, cómo se obtendría la evidencia y de qué manera se utilizaría para sustentar los hallazgos.

Tabla 1
Planificación del diagnostico de los controles de seguridad de la información

Elemento de planificación	Aplicación en el diagnóstico
Motivo	La revisión se realizó ante la necesidad de conocer la situación actual de los controles relacionados con la salvaguarda de los datos manejados en las actividades del Centro.
Objetivo	Examinar la situación actual de los controles relacionados con la salvaguarda de los datos e identificar las principales debilidades que servirían de base para la propuesta.
Alcance	La revisión comprendió políticas de seguridad, cuentas y autenticación, permisos de acceso, respaldo y recuperación, gestión de riesgos, auditoría y monitoreo de controles.
Aspectos por examinar	Se consideraron las prácticas relacionadas con el manejo de la información, los accesos, respaldos, responsabilidades, riesgos y evidencias disponibles sobre los controles incluidos en el diagnóstico.
Fuentes de información	Se consideró a la persona responsable del Centro, estudiantes de vinculación, docentes supervisores y la documentación y evidencia disponibles durante el estudio.
Procedimientos e instrumentos	Se planificó aplicar entrevista, encuesta, revisión documental, observación directa y lista de verificación, de acuerdo con el tipo de información requerida.

Criterios de revisión	La evidencia obtenida se contrastaría con los criterios técnicos y legales seleccionados para el estudio, únicamente dentro del alcance establecido.
Análisis previsto	Los resultados de los instrumentos serían comparados para identificar coincidencias, diferencias y evidencia suficiente para sustentar los hallazgos del diagnóstico.

Nota. La planificación corresponde al diagnóstico desarrollado en la investigación y no representa la aplicación del modelo de auditoría informática propuesto en el Capítulo III.

Una vez concluida la planificación, se procedió con la ejecución del diagnóstico mediante la aplicación de los instrumentos definidos. Los resultados obtenidos fueron posteriormente contrastados para la formulación y comunicación de los hallazgos.

2.7.2 Ejecución del proceso

Una vez establecidos los elementos de la planificación, se procedió con la ejecución mediante la aplicación de las técnicas e instrumentos definidos. Esta etapa comprendió la entrevista, la encuesta, la revisión documental, la observación directa y la lista de verificación, con el propósito de recopilar información y contrastar la evidencia disponible sobre los aspectos incluidos en la revisión.

2.7.2.1 Entrevista

La entrevista semiestructurada utiliza una guía de preguntas previamente definida y permite solicitar aclaraciones o ampliar respuestas relevantes durante su aplicación (Saunders et al., 2023). En esta investigación se empleó como fuente cualitativa de contexto para conocer, desde la perspectiva de la persona responsable, las prácticas de gestión de la información, los controles existentes y las necesidades identificadas en el Centro de Apoyo La U asesora.ec. Sus respuestas no se consideraron evidencia concluyente por sí solas, sino que fueron contrastadas con la encuesta, la revisión documental, la observación directa y el checklist.

2.7.2.1.1 Aplicación de la entrevista

La entrevista se aplicó a la persona responsable del Centro debido a su conocimiento de los procesos administrativos, tecnológicos y de gestión de la información. La guía abordó las políticas de seguridad, el control de accesos, los procedimientos de respaldo, la

capacitación, la realización de auditorías previas y las necesidades percibidas de mejora. Las respuestas se organizaron por temas y posteriormente se compararon con la evidencia obtenida mediante las demás técnicas. Los contenidos principales de la entrevista se resumen en la Tabla 1.

Tabla 2

Síntesis de las respuestas de la entrevista

Aspecto consultado	Síntesis de la respuesta
Políticas de seguridad de la información	La persona entrevistada indicó que el Centro no dispone de políticas de seguridad formalmente documentadas para orientar el manejo de la información institucional.
Control de acceso	Según lo señalado en la entrevista, en algunos procesos se emplean cuentas compartidas y no se dispone de un procedimiento documentado para administrar los usuarios.
Respaldo de información	Durante la entrevista se señaló que las copias de seguridad no se realizan periódicamente y que el Centro tampoco dispone de un plan formal de recuperación ante incidentes.
Capacitación	De acuerdo con la respuesta obtenida, el personal y los estudiantes de vinculación no reciben capacitaciones periódicas relacionadas con la seguridad de la información.
Auditorías informáticas	La persona entrevistada manifestó que no se habían realizado auditorías informáticas previas para revisar los controles de seguridad.
Necesidad de mejora	La persona responsable consideró necesaria la realización de una auditoría informática para fortalecer la protección de la información institucional.

Nota. Elaboración propia a partir de la entrevista semiestructurada aplicada a la persona responsable del Centro de Apoyo La U asesora.ec.

Las respuestas de la persona responsable destacaron algunas áreas que merecen una revisión adicional, como la formalización de políticas de seguridad, la gestión de usuarios y accesos, la frecuencia de los respaldos y la existencia de procedimientos de recuperación.

También se compartió que no se cuenta con capacitación periódica ni con auditorías informáticas previas. Al ser esta información proporcionada por un solo informante, se entiende más bien como una descripción de las prácticas declaradas, en lugar de una evidencia definitiva que confirme todas las condiciones mencionadas.

Estas declaraciones guiaron la revisión de documentos, la observación directa y el uso del checklist. Las condiciones respaldadas por la coincidencia entre las diferentes fuentes fueron posteriormente estructuradas como hallazgos de auditoría en el apartado 2.8. La valoración favorable de la persona responsable respecto de una auditoría informática evidencia una necesidad percibida dentro del Centro, pero no demuestra la eficacia del modelo propuesto, cuya implementación no formó parte del alcance de la investigación.

2.7.2.2 Encuesta

La encuesta se empleó como técnica de recolección de datos cuantitativos mediante un cuestionario estructurado (Saunders et al., 2023). Su propósito fue describir las respuestas de los participantes sobre cinco aspectos: conocimiento de las políticas de protección de datos, capacitación en seguridad informática, realización periódica de auditorías informáticas, cambio periódico de la contraseña de acceso y disponibilidad de copias de seguridad. Debido a que la información procede de respuestas declaradas, los resultados expresan percepciones y prácticas reportadas; por sí solos, no verifican la existencia ni la eficacia de los controles de seguridad.

2.7.2.2.1 Aplicación de la Encuesta

El cuestionario fue administrado a los 40 integrantes de la población objeto de estudio a través de Google Forms: 36 estudiantes de vinculación y 4 docentes supervisores del Centro de Apoyo La U asesora.ec. Dado que se realizó una aplicación de censo, no fue necesario seleccionar una muestra. La persona entrevistada, responsable, proporcionó información cualitativa de manera independiente y no formó parte de los 40 participantes.

Las respuestas se organizaron en frecuencias y porcentajes y se compararon con los resultados de la entrevista, del análisis de documentos y de la lista de verificación de auditoría de TI. Esta integración nos permitió establecer una clara distinción entre las percepciones de los participantes y la evidencia de los controles evaluados.

Tabla 3
Conocimiento de las políticas de protección de datos

Respuesta	Frecuencia	Porcentaje
Siempre	4	10%
Casi siempre	6	15%
Algunas veces	8	20%
Rara vez	10	25%
Nunca	12	30%
Total	**40**	**100%**

Nota. Elaboración propia a partir de la encuesta administrada mediante Google Forms a 40 participantes del Centro de Apoyo La U asesora.ec.

Los resultados muestran un bajo nivel de conocimiento declarado sobre las políticas de protección de datos, ya que el 55 % de los participantes se concentró en las categorías “Rara vez” y “Nunca”. Esta tendencia evidencia la necesidad de fortalecer la comunicación y socialización de las directrices relacionadas con la protección de datos entre los participantes del Centro.

Este resultado no indica, por sí solo, que las políticas no existan ni que se hayan violado controles. Sin embargo, resalta una brecha en el conocimiento, la cual debe ser confirmada mediante entrevistas, análisis de documentos y el checklist de auditoría informática. La verificación de políticas aprobadas, mecanismos de difusión y registros de capacitación permitirá determinar si el problema corresponde a falta de formalización, comunicación insuficiente o ambas situaciones.

Tabla 4
Capacitación en seguridad informática

Respuesta	Frecuencia	Porcentaje
Siempre	2	5%
Casi siempre	2	5%
Algunas veces	8	20%
Rara vez	14	35%
Nunca	14	35%
Total	**40**	**100%**

Nota. Elaboración propia a partir de la encuesta administrada mediante Google Forms a 40 participantes del Centro de Apoyo La U asesora.ec.

De los 40 participantes, 28 (70 %) indicaron que rara vez o nunca habían recibido capacitación en seguridad informática. Ocho encuestados (20 %) seleccionaron “Algunas veces”, mientras que únicamente 4 (10 %) eligieron “Siempre” o “Casi siempre”. La distribución muestra que, para la mayoría de los estudiantes de vinculación y docentes supervisores, la capacitación no fue percibida como una actividad recurrente.

Por tratarse de información declarada, este resultado no demuestra por sí solo que el Centro carezca de un programa formal ni permite medir las competencias de los participantes. Para determinar si existe una debilidad de control, debe verificarse la disponibilidad de cronogramas, contenidos, materiales y registros de asistencia o evaluación. Si el análisis documental confirma la falta de estas evidencias, el resultado respaldará la incorporación de actividades periódicas de capacitación dentro de la propuesta.

Tabla 5

Realización periódica de auditorías informáticas

Respuesta	Frecuencia	Porcentaje
Siempre	30	75%
Casi siempre	8	20%
Algunas veces	2	5%
Rara vez	0	0%
Nunca	0	0%

Total	**40**	**100%**

Nota. Elaboración propia a partir de la encuesta administrada mediante Google Forms a 40 participantes del Centro de Apoyo La U asesora.ec.

Ante el ítem relacionado con la importancia de realizar auditorías informáticas periódicas, 30 participantes (75 %) seleccionaron “Siempre” y 8 (20 %) eligieron “Casi siempre”. Los 2 participantes restantes (5 %) respondieron “Algunas veces”, mientras que las categorías “Rara vez” y “Nunca” no registraron respuestas. En general, la mayoría de los encuestados, 38 de 40, se inclinó hacia las dos categorías más altas, reflejando una percepción muy positiva sobre este tipo de evaluación.

Este resultado expresa la valoración de los estudiantes de vinculación y de los docentes supervisores, pero no demuestra que el Centro haya realizado auditorías con anterioridad. De hecho, la entrevista y la revisión documental no identificaron informes, planes ni registros de auditorías informáticas previas. La encuesta permite establecer que los participantes reconocen su importancia, mientras que la evidencia documental confirma la necesidad de formalizar su planificación y su ejecución.

Tabla 6

Cambio periódico de la contraseña de acceso

Respuesta	**Frecuencia**	**Porcentaje**
Siempre	2	5%
Casi siempre	6	15%
Algunas veces	12	30%
Rara vez	13	32,5%
Nunca	7	17,5%
Total	**40**	**100%**

Nota. Esta es una elaboración propia, basada en una encuesta realizada a través de Google Forms a 40 participantes del Centro de Apoyo La U asesora.ec.

De los 40 participantes, 20 (50 %) indicaron que rara vez o nunca cambian su contraseña de acceso. Doce encuestados (30 %) seleccionaron “Algunas veces” y los 8 restantes (20 %) respondieron “Siempre” o “Casi siempre”. Estos valores describen la frecuencia declarada de cambio, pero no permiten determinar por sí solos si las contraseñas utilizadas son seguras ni si el mecanismo de autenticación es adecuado.

NIST SP 800-63B-4 señala que los verificadores no deben exigir cambios periódicos de contraseña y que deben forzar su modificación cuando exista evidencia de compromiso (Temoshok et al., 2025). En el Centro, la valoración de este control también debe considerar la longitud de las contraseñas, la detección de credenciales comprometidas, el uso de cuentas compartidas y la autenticación multifactor. Por ello, el resultado de la encuesta justifica revisar la gestión integral de la autenticación, pero no imponer automáticamente una renovación cada cierto número de días.

Tabla 7

Frecuencia de realización de copias de seguridad

Respuesta	Frecuencia	Porcentaje
Siempre	8	20%
Casi siempre	6	15%
Algunas veces	14	35%
Rara vez	12	30%
Nunca	0	0%
Total	**40**	**100%**

Nota. Elaboración propia basada en la encuesta administrada a 40 participantes del Centro de Apoyo La U asesora.ec, mediante la plataforma Google Forms.

De los 40 participantes, 14 (35 %) indicaron que siempre o casi siempre realizan copias de seguridad, mientras que otros 14 (35 %) dijeron que lo hacen algunas veces, y 12 (30 %) respondieron que rara vez lo hacen. Ninguno mencionó que nunca lo hagan. Esto significa que

el 65 % de los encuestados perciben esta práctica como algo intermedio o poco frecuente, reflejando una realización irregular desde la perspectiva de quienes participan en las actividades del Centro.

Por otro lado, la encuesta no puede confirmar si las copias son completas ni si realmente existe la posibilidad de recuperar la información en caso de ser necesario. Para entender mejor el control de las copias, sería ideal revisar el procedimiento aprobado, quiénes son responsables, qué abarca, con qué frecuencia se hacen, cómo se almacenan, cómo se protegen las copias, las bitácoras de cada proceso y las pruebas de restauración, siguiendo las recomendaciones de ISO/IEC 27002:2022 (ISO, 2022b). La revisión de los documentos no encontró estas evidencias, por lo que parece que aún hay un importante trabajo por hacer para formalizar y seguir mejor el proceso de respaldo, sin que esto signifique que nunca se hayan realizado respaldos.

2.7.2.2.2 Análisis general de la encuesta

Los resultados muestran tres aspectos que requieren especial atención. El 55 % de los participantes seleccionó “Rara vez” o “Nunca” respecto al conocimiento de las políticas de protección de datos; el 70 % ubicó en esas mismas categorías la capacitación recibida y el 65 % señaló que las copias de seguridad se realizan algunas veces o rara vez. En cuanto al cambio de contraseñas, el 50 % respondió “Rara vez” o “Nunca”; sin embargo, este valor no constituye por sí solo una deficiencia, porque la seguridad del mecanismo depende también de la longitud de las contraseñas, de la existencia de cuentas compartidas, de la detección de credenciales comprometidas y de la autenticación multifactor. En lo que respecta al apartado de auditorías informáticas, el 95 % de las respuestas se concentró en las dos categorías superiores; dicha interpretación como una valoración favorable deberá mantenerse únicamente en aquellos casos en que coincida con la formulación original de la pregunta del cuestionario.

Estas respuestas muestran cómo vemos las cosas y las áreas en las que podemos mejorar en la comunicación de políticas, la capacitación y la formalización de respaldos. También se encontró que coinciden con las entrevistas, el análisis de documentos y los hallazgos de la lista de verificación, que reflejan problemas similares con los que estamos trabajando, lo que nos ayudó a entender mejor la situación. También encontramos que, aunque hay una buena percepción general de las auditorías, necesitamos contar con más evidencia en informes o registros para confirmar si se han realizado previamente. Esta información nos será muy útil para orientar los próximos pasos en el apartado 2.8 y definir algunos requisitos importantes para la propuesta, como contar con políticas escritas, mejorar la capacitación, gestionar mejor la autenticación, fortalecer los procedimientos de respaldo y planear las auditorías con mayor precisión, siempre con la certeza de que todo ello esté en marcha o haya sido revisado previamente.

2.7.2.3 Análisis documental y la lista de verificación (checklist) de auditoría informática

El análisis documental se utilizó para examinar políticas, inventarios, registros, bitácoras, configuraciones y otros documentos disponibles en el Centro de Apoyo La U asesora.ec, con el propósito de contrastarlos con criterios previamente establecidos (Saunders et al., 2023). A diferencia de la entrevista y la encuesta, que recopilaron declaraciones y percepciones, esta técnica permitió comprobar si existían registros que respaldaran las prácticas informadas por los participantes.

La revisión se realizó con un checklist de 40 ítems, organizado en las categorías “Cumple”, “Cumple parcialmente”, “No cumple” y “No aplicaLos criterios del instrumento estaban relacionados con los requisitos de la norma ISO/IEC 27001:2022, las directrices de control de la norma ISO/IEC 27002:2022 y las obligaciones pertinentes de la Ley Orgánica de Protección de Datos Personales (ISO, 2022b, 2022c; Asamblea Nacional de Ecuador, 2021).

Cada calificación iba acompañada de una breve descripción de la documentación revisada, la observación realizada y la configuración examinada.

La lista de verificación organizaba los resultados, y la evidencia se basaba en documentos, registros y observaciones que respaldaban cada respuesta. Estas evidencias se compararon con la entrevista y la encuesta para identificar coincidencias o diferencias entre lo dicho y lo comprobado. Los hallazgos formales derivados de esta integración se presentan en el apartado 2.8, estructurados en condición, criterio, causa, efecto, evidencia y recomendación.

2.7.2.3.1 Aplicación del checklist de auditoría informática

Tabla 8

Síntesis de los resultados del checklist de auditoría informática

Área Evaluada	Resultado resumido	Evidencia sintetizada
Políticas de seguridad de la información	No cumple	No se localizó una política, manual o documento institucional aprobado que estableciera lineamientos de seguridad de la información.
Gestión de activos de información	Cumple parcialmente	Se localizaron inventarios básicos de equipos y activos, pero no estaban actualizados ni incluían una clasificación de la criticidad de la información.
Gestión de usuarios y contraseñas	No cumple	Se identificaron cuentas compartidas, y no se encontró un procedimiento documentado para crear, modificar, revisar o retirar cuentas de usuario.
Control de acceso a la información	No cumple	No pudimos localizar una matriz de roles y permisos, y también notamos que los accesos a carpetas y recursos compartidos son bastante amplios.
Respaldo y almacenamiento de información	No cumple	No se encontraron cronogramas, bitácoras ni pruebas de restauración, y también notamos que se utilizaban plataformas personales para almacenar información institucional. Esto nos ayuda a entender mejor la situación y buscar soluciones juntos.

Área Evaluada	Resultado resumido	Evidencia sintetizada
Gestión de incidentes	No cumple	No se encontraron canales formales de reporte, registros de incidentes ni documentación de acciones correctivas.
Capacitación y protección de datos personales	No cumple	No se localizaron registros de capacitación, avisos de privacidad ni documentos que evidenciaran la información proporcionada a los titulares sobre el tratamiento de sus datos.
Seguridad física del área de servidores	Cumple	Se verificó que el área cuenta con acceso restringido y con medidas básicas de protección física.

Nota: elaboración propia basada en el listado de 40 ítems utilizado en el Centro de Apoyo La U asesora.ec. Los criterios del instrumento se alinearon con ISO/IEC 27001:2022, ISO/IEC 27002:2022 y con las disposiciones pertinentes de la Ley Orgánica de Protección de Datos Personales. El instrumento completo figura como el Instrumento N.º 3 en los anexos.

La síntesis muestra que en las áreas revisadas la mayoría de las calificaciones son "No cumple". Entre las condiciones más habituales se encuentran la ausencia de políticas documentadas, el uso de cuentas compartidas, la falta de una matriz de roles y permisos, la formalización insuficiente de los respaldos y la ausencia de registros para la gestión de incidentes. El inventario de activos presenta un cumplimiento parcial, ya que dispone de registros básicos que no están actualizados ni consideran criterios de criticidad.

El acceso restringido al área de servidores fue el único resultado favorable incluido en la tabla. Este control físico es pertinente, pero no permite generalizar que toda la seguridad física o la gestión de la información sea adecuada. Los resultados resumidos orientaron la formulación de los hallazgos del apartado 2.8, los cuales solo se consideraron sustentados cuando la condición observada pudo relacionarse con un criterio aplicable y con evidencia específica.

2.7.3 Comunicación de resultados

Una vez concluida la ejecución, la información obtenida mediante la entrevista, la encuesta, el análisis documental y la lista de verificación fue contrastada para determinar las

principales condiciones identificadas en el Centro. Los resultados se organizaron en seis hallazgos, estructurados mediante condición, criterio, causa, efecto o riesgo, evidencia y recomendación. Esta forma de presentación permitió relacionar cada situación detectada con su sustento y establecer las acciones de mejora correspondientes. En conjunto, los hallazgos constituyen la síntesis de los resultados del diagnóstico y sirven de base para el desarrollo de la propuesta presentada en el Capítulo III.

2.7.3.1 Hallazgos de auditoría identificados

Hallazgo 1. Política de seguridad de la información no formalizada

Condición. Entre los documentos puestos a disposición durante la revisión no se localizó una política de seguridad de la información aprobada por la autoridad competente y aplicable al Centro de Apoyo La U asesora.ec. Tampoco se encontró evidencia de lineamientos formalmente comunicados, de asignación de responsabilidades ni de una periodicidad establecida para su revisión.

Criterio. La cláusula 5.2 de ISO/IEC 27001:2022. Establece que la alta dirección debe definir y comunicar una política de seguridad de la información y mantenerla como información documentada. El control 5.1 de ISO/IEC 27002:2022 aborda aspectos relativos a su aprobación, comunicación, disponibilidad y revisión planificada (ISO, 2022b, 2022c).

Causa. No se identificó un mecanismo formal para adoptar en el Centro las políticas institucionales de la ULEAM ni una persona responsable de coordinar su aplicación, comunicación y seguimiento.

Efecto o riesgo. La ausencia de lineamientos aplicables al Centro puede ocasionar que los controles se ejecuten con criterios distintos y sin responsabilidades claramente asignadas. Esta situación dificulta mostrar una gestión sólida de la seguridad de la información y mantener un seguimiento cercano de las medidas que hemos puesto en marcha.

Evidencia. El ítem 1 del checklist fue calificado como “No cumple”. Durante la revisión, no se presentó ninguna política, manual, reglamento ni documento aprobado que estableciera los lineamientos de seguridad para el Centro. Además, la persona entrevistada mencionó que no existía una política formalmente documentada.

Recomendación. Sería recomendable que la autoridad competente de la ULEAM revise si existe una política institucional de seguridad de la información vigente para el Centro. En caso afirmativo, sería importante formalizar su adopción, comunicarla y realizar un seguimiento adecuado. Si no existe, sería conveniente gestionar su elaboración y aprobación a nivel institucional. En cualquier situación, sería útil definir claramente el alcance, asignar una persona responsable, comunicar los lineamientos a los docentes y estudiantes vinculados, conservar evidencia de su recepción y establecer un calendario de revisiones periódicas.

Hallazgo 2. Uso de cuentas compartidas y controles de autenticación insuficientes

Condición. Durante la observación, se detectó que se está utilizando una cuenta genérica o compartida para acceder a los equipos y recursos del Centro. Además, en la documentación revisada no se encontró ningún procedimiento que detallara cómo se asignan las cuentas individuales, los requisitos para proteger la información de autenticación, la revisión de cuentas activas, la desactivación de accesos o las acciones a seguir en caso de que una credencial se vea comprometida. Es importante contar con estos procedimientos para garantizar una mayor seguridad y organización.

Criterio. Los controles 5.16 y 5.17 de ISO/IEC 27002:2022 establecen orientaciones para la gestión del ciclo de vida de las identidades y la protección de la información de autenticación. NIST SP 800-63B-4 incorpora requisitos sobre la longitud de las contraseñas, el bloqueo de valores comunes o comprometidos y el cambio cuando exista evidencia de compromiso; además, contempla el uso de autenticación multifactor según el nivel de aseguramiento requerido (ISO, 2022b; Temoshok et al., 2025).

Causa. No se encontró una responsabilidad claramente definida para administrar las cuentas en el Centro, ni un procedimiento coordinado con el área tecnológica de la ULEAM para gestionar su creación, modificación, revisión y desactivación. Esto puede facilitar una mejor gestión y seguridad de las cuentas.

Efecto o riesgo. El uso compartido de una identidad de acceso puede dificultar identificar quién realizó cada acción, lo que puede generar confusión. Además, complica el proceso de retirar permisos de forma individual y aumenta el riesgo de accesos no autorizados o de uso indebido de los recursos de la institución. Es importante contar con medidas que aseguren que cada usuario tenga su propia identidad para mantener todo más seguro y claro.

Evidencia. Los ítems 4 y 5 del checklist fueron calificados como "No cumple" debido a la falta de cuentas individualizadas y al uso de accesos compartidos. Durante la revisión se identificó una cuenta genérica de inicio de sesión. Además, el ítem 6 fue valorado como "Cumple parcialmente", mientras que el ítem 9 obtuvo la calificación de "No cumple", debido a que no existe un proceso definido para desactivar accesos.

Recomendación. Se recomienda coordinar con el equipo de tecnología de la ULEAM el reemplazo gradual de las cuentas compartidas por usuarios individuales. También es necesario elaborar un inventario de cuentas y dejar constancia de las solicitudes, autorizaciones, cambios, revisiones y desactivaciones realizadas.

En caso de que sea necesario mantener una cuenta compartida o de servicio, se debe definir su propósito, responsable, usuarios autorizados y forma de seguimiento. Además, las contraseñas deben cumplir con las prácticas de seguridad establecidas y cambiarse cuando exista sospecha o evidencia de compromiso.

Hallazgo 3. Permisos de acceso sin matriz de roles ni revisión periódica

Condición. En la documentación puesta a disposición no se encontró una matriz que vincule las funciones del personal con los recursos y los niveles de acceso autorizados. Asimismo,

durante la revisión de los permisos de un directorio compartido de la red institucional, se observaron accesos más amplios de los requeridos por las funciones, sin evidencia documental de su aprobación ni de su revisión periódica.

Criterio. Los controles 5.15, 5.18 y 8.2 de ISO/IEC 27002:2022 contemplan la definición de reglas de acceso, la asignación y revisión de los derechos concedidos y la restricción de los privilegios elevados. De manera complementaria, los controles AC-3 y AC-6 de NIST SP 800-53 Rev. 5 establecen la aplicación de las autorizaciones aprobadas y el principio de mínimo privilegio (ISO, 2022b; Joint Task Force, 2020).

Causa. No se evidenció un procedimiento formal que vinculara las funciones, los recursos institucionales, los permisos requeridos y las personas responsables de aprobarlos. Tampoco se presentó un mecanismo documentado para revisar periódicamente los accesos concedidos.

Efecto o riesgo. La permanencia de permisos superiores a los necesarios podría facilitar la modificación, eliminación o divulgación no autorizada de información institucional. Esta situación también dificultaría determinar responsabilidades por una operación indebida sobre los recursos compartidos.

Evidencia. Los ítems 8 y 10 del checklist fueron calificados como «No cumple», mientras que el ítem 11 obtuvo la valoración «Cumple parcialmente». Además, la revisión de los permisos de un directorio compartido mostró accesos amplios, sin registro de aprobación ni de revisión.

Recomendación. Elabora, junto con la unidad responsable de tecnologías de la información de la ULEAM, una matriz sencilla que indique quién tiene qué rol, qué recursos puede usar, su nivel de permiso, quién es la persona responsable y quién aprueba el acceso. Con esta matriz, es recomendable retirar los permisos que ya no corresponden a las funciones, guardar evidencia de las autorizaciones y revisar los accesos de manera periódica, especialmente cuando cambien las funciones, haya desvinculaciones o se incorporen nuevos recursos.

Hallazgo 4. Respaldo y recuperación de información sin procedimiento formal

Condición. Durante la revisión no se presentaron cronogramas ni bitácoras que permitieran comprobar la periodicidad y ejecución de las copias de seguridad. Además, no se encontraron procedimientos escritos para recuperar la información ante un incidente, ni registros de pruebas de restauración o evidencia de un repositorio alterno autorizado.

Criterio. El control 8.13 de ISO/IEC 27002:2022 establece que las copias de la información, el software y los sistemas deben mantenerse y probarse regularmente conforme a una política de respaldo. A su vez, el control 5.30 orienta a planificar, mantener y comprobar la preparación de las tecnologías de la información y la comunicación frente a interrupciones que puedan afectar la continuidad de las operaciones (ISO, 2022b).

Causa. La gestión de los respaldos no está formalizada en un documento que establezca la información incluida, la periodicidad de las copias, los repositorios institucionales autorizados, los responsables, el plazo de conservación y el mecanismo para comprobar su recuperación.

Efecto o riesgo. Ante una eliminación accidental, una falla tecnológica, un incidente de seguridad o el daño de un equipo, la falta de respaldos comprobables podría ocasionar la pérdida de información y prolongar la interrupción de las actividades del Centro. Asimismo, no sería posible saber de antemano si las copias disponibles podrían restaurarse íntegramente.

Evidencia. Los ítems 17, 18, 19 y 20 del checklist fueron calificados como «No cumple». En ellos se registró la falta de cronogramas y bitácoras de ejecución, de un repositorio alterno autorizado, de informes de pruebas de restauración y de un procedimiento documentado para recuperar la información ante pérdidas o incidentes.

Recomendación. Junto con el departamento de TI de ULEAM, podemos desarrollar un procedimiento para respaldar y recuperar la información y solicitar la aprobación de la autoridad. Este documento debe detallar claramente qué información se respalda, con qué frecuencia, cuánto tiempo se conserva y quién es responsable, quiénes son los repositorios

autorizados, cómo se protegen las copias y cómo se prueban las restauraciones. Además, cada respaldo y cada prueba deben registrarse para garantizar futuras verificaciones y correcciones.

Hallazgo 5. Gestión de riesgos de seguridad de la información no documentada

Condición. En la documentación examinada no se localizó una matriz ni otro registro que demostrara la aplicación de un proceso de evaluación de riesgos de seguridad de la información. En particular, no se presentó un análisis que relacionara los activos utilizados por el Centro con las amenazas, vulnerabilidades y consecuencias potenciales que podrían afectarlos.

Criterio. Las cláusulas 6.1.2 y 6.1.3 de ISO/IEC 27001:2022 establecen requisitos para la evaluación y el tratamiento de los riesgos de seguridad de la información (ISO, 2022c). Además, la gestión de riesgos puede apoyarse en la ISO/IEC 27005:2022, ya que esta norma orienta su evaluación, tratamiento, comunicación, seguimiento y revisión (ISO, 2022a).

Causa. El Centro aún no dispone de una metodología documentada que establezca cómo valorar la probabilidad y el impacto de los riesgos, quiénes participan en su evaluación y con qué frecuencia deben revisarse. Como resultado, se dificulta el análisis y seguimiento de las debilidades identificadas, porque no se registran con criterios uniformes.

Efecto o riesgo. Cuando no se realiza una evaluación ordenada de los riesgos, las decisiones de seguridad pueden tomarse solo para resolver problemas inmediatos. Esto impide analizar antes qué tan probable es que ocurra un riesgo y qué impacto podría tener en las actividades del Centro. Debido a esto, se vuelve más difícil definir qué riesgos deben atenderse primero, qué controles son más necesarios y en qué aspectos conviene usar los recursos disponibles.

Evidencia. Durante la revisión no se encontró una matriz de riesgos de TI ni un análisis documentado que relacionara los activos de información con posibles amenazas, vulnerabilidades e impactos. Por esta razón, el ítem 38 de la lista de verificación fue calificado como “No cumple”.

Recomendación. Se recomienda trabajar junto con la unidad de tecnología de la información de la ULEAM para elaborar una metodología y un registro que permitan gestionar los riesgos de seguridad de la información. En este registro se debe incluir, como mínimo, el activo o proceso afectado, la amenaza, la vulnerabilidad, las posibles consecuencias, la probabilidad, el impacto, el nivel de riesgo, los controles existentes, las acciones de tratamiento, el responsable y la fecha de revisión.

Después de aplicar las acciones correspondientes, se deberá revisar el riesgo restante y dejar documentada la decisión tomada por la instancia institucional competente.

Hallazgo 6. Ausencia de auditorías internas y de monitoreo sistemático de los controles.

Condición. Durante la revisión de la documentación, no se encontraron planes, programas ni informes que evidenciaran auditorías de TI anteriores en el Centro de Soporte. Tampoco se hallaron registros sobre revisiones periódicas de controles, indicadores de desempeño, actas de seguimiento o responsables de comprobar su efectividad.

Criterio. Como criterios de referencia, las cláusulas 9.1, 9.2 y 9.3 de ISO/IEC 27001:2022 contemplan el seguimiento y la evaluación del desempeño, la ejecución de auditorías internas a intervalos planificados y la revisión del sistema por parte de la dirección. Por su parte, ISO 19011:2026 proporciona directrices sobre los principios de auditoría, la gestión del programa, la realización de las auditorías y la competencia de las personas participantes (ISO, 2022c, 2026).

Causa. No hay un ciclo claro y documentado de evaluación que ayude a identificar quiénes son los responsables, cuáles son los criterios, con qué frecuencia se realiza, qué documentos se requieren y cuál es el procedimiento para dar seguimiento a las acciones que surgen de cada revisión.

Efecto o riesgo. La falta de evaluaciones periódicas puede hacer que las deficiencias en los controles pasen desapercibidas o que las acciones acordadas no se verifiquen con facilidad.

Además, esto dificultaría contar con evidencia suficiente para confirmar si las medidas adoptadas efectivamente resuelven los problemas detectados.

Evidencia. Los ítems 37, 39 y 40 del listado fueron evaluados como «No cumple». El ítem 37 indica la ausencia de responsables designados para la revisión de la eficacia de los controles; el ítem 39 señala la inexistencia de informes de gestión, actas de revisión ni indicadores de seguridad; y el ítem 40 evidencia la falta de planes o informes finales de auditorías informáticas previas.

Recomendación. Se recomienda trabajar junto con la autoridad institucional y el equipo de tecnología de la información de la ULEAM para aplicar auditorías o evaluaciones de TI de forma periódica, considerando los riesgos existentes. Para ello, el programa debe establecer el objetivo, alcance, criterios, frecuencia, responsables y la forma en que se comunicarán los hallazgos.

Cuando se identifiquen hallazgos que necesiten corrección, estos deben relacionarse con acciones de mejora, una persona responsable, un plazo definido y la evidencia que permita comprobar su cierre. El modelo presentado en el Capítulo III puede usarse como referencia para una prueba piloto, previa autorización institucional, y luego ser evaluado según los resultados obtenidos.

CAPÍTULO III

3. DISEÑO DE LA PROPUESTA

3.1 Título

Guía de seguridad de la información para fortalecer la salvaguarda de los datos en el Centro de Apoyo La U asesora.ec.

3.2 Justificación

La elaboración de la guía se sustenta en los resultados obtenidos durante el diagnóstico realizado en el Centro de Apoyo La U Asesor@.ec. La entrevista, la encuesta, el análisis documental y la lista de verificación permitieron identificar debilidades relacionadas con la formalización de políticas de seguridad de la información, la gestión de cuentas y permisos de acceso, los procedimientos de respaldo y recuperación, la gestión de riesgos y el seguimiento periódico de los controles. Estos resultados evidencian la necesidad de contar con lineamientos claros que orienten el manejo y protección de la información utilizada en las actividades del Centro.

La guía busca responder a estas necesidades mediante lineamientos, procedimientos y formatos que faciliten la organización de las prácticas de seguridad de la información. Su contenido se orienta a establecer responsabilidades, mejorar la gestión de accesos, organizar los respaldos y la recuperación de información, apoyar la identificación y tratamiento de riesgos y promover la revisión periódica de los controles. Para su elaboración se consideran los criterios técnicos y legales aplicables al alcance de la propuesta, sin que su utilización implique la implementación o certificación de un sistema de gestión de seguridad de la información.

3.3 Objetivos

3.3.1 Objetivo general

Establecer lineamientos y procedimientos de seguridad de la información que orienten la protección de los datos y contribuyan a fortalecer los controles aplicables en el Centro de Apoyo La U asesora.ec.

3.3.2 Objetivos específicos

- Establecer lineamientos de seguridad de la información que definan responsabilidades y orienten el manejo y protección de los datos en el Centro.
- Definir procedimientos para la gestión de cuentas, autenticación, roles y permisos de acceso, de acuerdo con las necesidades identificadas en el diagnóstico.
- Establecer procedimientos para el respaldo, recuperación y protección de la información utilizada en las actividades del Centro.
- Incorporar mecanismos para la identificación, valoración, tratamiento y seguimiento de los riesgos relacionados con la seguridad de la información.
- Establecer mecanismos de revisión y seguimiento de los controles, las acciones de mejora, los responsables, los plazos y las evidencias de cumplimiento.

3.4 Alcance

La propuesta comprende una guía de seguridad de la información dirigida al Centro de Apoyo La U Asesora.ec, elaborada a partir de las necesidades identificadas durante el diagnóstico. Su contenido incluye lineamientos relacionados con responsabilidades y manejo de la información, gestión de cuentas y accesos, roles y permisos, respaldo y recuperación de datos, gestión de riesgos, así como mecanismos de revisión y seguimiento de los controles.

La guía tiene un alcance documental y está orientada a servir como apoyo para organizar y fortalecer las prácticas de seguridad de la información del Centro. Su desarrollo no contempla la implementación inmediata de los controles, modificaciones en cuentas o configuraciones tecnológicas, pruebas de penetración, análisis forense ni cambios en la infraestructura institucional. Su futura aplicación estará sujeta a la autorización de la ULEAM y a las condiciones y responsabilidades institucionales correspondientes.

3.5Base legal

3.5.1 Constitución de la Republica del Ecuador

El artículo 66, numeral 19, reconoce el derecho de las personas a decidir sobre el uso de sus datos personales y establece condiciones para su recopilación, archivo, procesamiento, distribución o difusión. Este principio sustenta la necesidad de mantener un manejo responsable de la información utilizada en las actividades del Centro y sirve como fundamento jurídico para los lineamientos planteados en la guía (Constitución de la República del Ecuador, 2008, art. 66, núm. 19).

3.5.2 Ley Orgánica de Protección de Datos Personales

La Ley Orgánica de Protección de Datos Personales establece principios que deben observarse durante el tratamiento de datos personales y dispone la adopción de medidas de seguridad adecuadas para prevenir riesgos relacionados con su tratamiento. Estas disposiciones se consideran en la guía para orientar el manejo de la información, la asignación de responsabilidades y la aplicación de medidas que contribuyan a reducir accesos, usos o tratamientos no autorizados (Asamblea Nacional del Ecuador, 2021, arts. 10, 37).

3.5.3 Reglamento General de la Ley Orgánica de Protección de Datos Personales

Expedido mediante el Decreto Ejecutivo No. 904, este instrumento complementa las disposiciones de la LOPDP y sirve de referencia para establecer responsabilidades y medidas

aplicables al manejo de información personal dentro del Centro (Presidencia de la República del Ecuador, 2023).

3.5.4 ISO/IEC 27001:2022

La ISO/IEC 27001:2022 se considera como referente técnico para orientar los lineamientos de la guía relacionados con la gestión de accesos, responsabilidades, riesgos y protección de la información. Su utilización permite organizar estos aspectos de acuerdo con las necesidades identificadas en el diagnóstico, sin que ello implique la implementación o certificación de un sistema de gestión de seguridad de la información (ISO, 2022c).

3.5.5 ISO/IEC 27002:2022

La ISO/IEC 27002:2022 aporta orientaciones para la aplicación de controles de seguridad de la información. En la guía se utiliza como referente para establecer medidas relacionadas con la gestión de accesos, autenticación, responsabilidades, respaldos y otras prácticas vinculadas con las necesidades identificadas en el Centro (ISO, 2022b).

3.5.6 ISO/IEC 27005:2022

La ISO/IEC 27005:2022 se toma como referencia para orientar la gestión de los riesgos asociados con la seguridad de la información. Su aplicación en la guía permite organizar la identificación, valoración y tratamiento de los riesgos, así como establecer responsables y acciones de seguimiento de acuerdo con las condiciones identificadas en el Centro (ISO, 2022a).

3.6 Desarrollo de la propuesta

3.6.1 Presentación de la guía

La propuesta está organizada en cinco componentes que abarcan los principales aspectos identificados durante el diagnóstico: lineamientos de seguridad, gestión de accesos, respaldo y recuperación, gestión de riesgos, y revisión y seguimiento. En cada componente se

establecen orientaciones y herramientas de apoyo para facilitar su aplicación en las actividades del Centro.

3.6.2 Componentes estratégicos y organizativos

El diagnóstico evidenció que el Centro no cuenta con misión, visión y valores propios formalmente documentados. Por esta razón, se plantean estos elementos como apoyo a su organización interna, junto con una estructura funcional que permita identificar responsabilidades relacionadas con el manejo de la información. Su adopción estará sujeta a la revisión y aprobación de la autoridad institucional correspondiente.

3.6.2.1 Misión propuesta

La misión propuesta delimita el propósito del Centro, sus beneficiarios, los servicios documentados en el diagnóstico y la participación de docentes y estudiantes. También se destaca la importancia de proteger la información, considerándola un aspecto clave en todas las actividades de asesoría y acompañamiento.

La misión propuesta del Centro es brindar apoyo gratuito a emprendedores y organizaciones de El Carmen y sus zonas cercanas, mediante capacitaciones, asesorías y acompañamiento técnico en emprendimiento y gestión de negocios. Estas actividades se desarrollarán con la participación de docentes y estudiantes de la Universidad Laica Eloy Alfaro de Manabí, Extensión El Carmen, promoviendo la ética, la calidad, la confidencialidad y el manejo responsable de la información.

3.6.2.2 Visión propuesta

La visión propuesta establece el estado al que aspira el Centro de Apoyo La U asesora.ec al finalizar el periodo de ejecución documentado en el apartado 2.2. Su formulación conserva el carácter universitario del proyecto y vincula su reconocimiento con la calidad de los servicios prestados, la participación de docentes y estudiantes y el manejo responsable de

la información. Al igual que los demás componentes del direccionamiento estratégico, su adopción está sujeta a la revisión y aprobación de la autoridad competente de la ULEAM.

Al término de su periodo de ejecución, previsto para enero de 2029, consolidarse como un espacio de vinculación de la Universidad Laica Eloy Alfaro de Manabí, reconocido en El Carmen y su zona de influencia, por la calidad de los servicios de asesoría, capacitación y acompañamiento técnico dirigidos a emprendedores y organizaciones, la participación formativa de docentes y estudiantes y el manejo responsable de la información.

3.6.2.3 Valores propuestos

Los valores propuestos orientan la actuación de las personas que participan en las actividades del Centro y complementan los principios institucionales de la ULEAM.

Tabla 8

Propuesta de valores corporativos para el Centro de Apoyo La U Asesora.ec

Valor	Descripción
Ética	Actuar con honestidad y respeto durante la atención a los usuarios, el manejo de la información y la elaboración de los productos de asesoría.
Responsabilidad	Responsabilidad: Consiste en cumplir adecuadamente con las tareas asignadas, cuidar las evidencias de las actividades realizadas y utilizar de forma correcta la información y las herramientas entregadas.
Confidencialidad	Se refiere al manejo cuidadoso de la información institucional y de los datos personales, compartiéndolos solo cuando sea necesario para el desarrollo del proyecto.
Compromiso	Implica participar activamente en las actividades de consultoría, capacitación y seguimiento a los usuarios, manteniendo una comunicación clara entre docentes, estudiantes y la dirección.
Innovación	Evaluar y adoptar, cuando sea pertinente y exista autorización institucional, herramientas tecnológicas que contribuyan a mejorar los servicios y la gestión de la información. Su incorporación deberá responder a las necesidades del Centro y apoyar la mejora de sus procesos.

Nota. Elaboración propia a partir del diagnóstico del Centro de Apoyo La U asesora.ec.

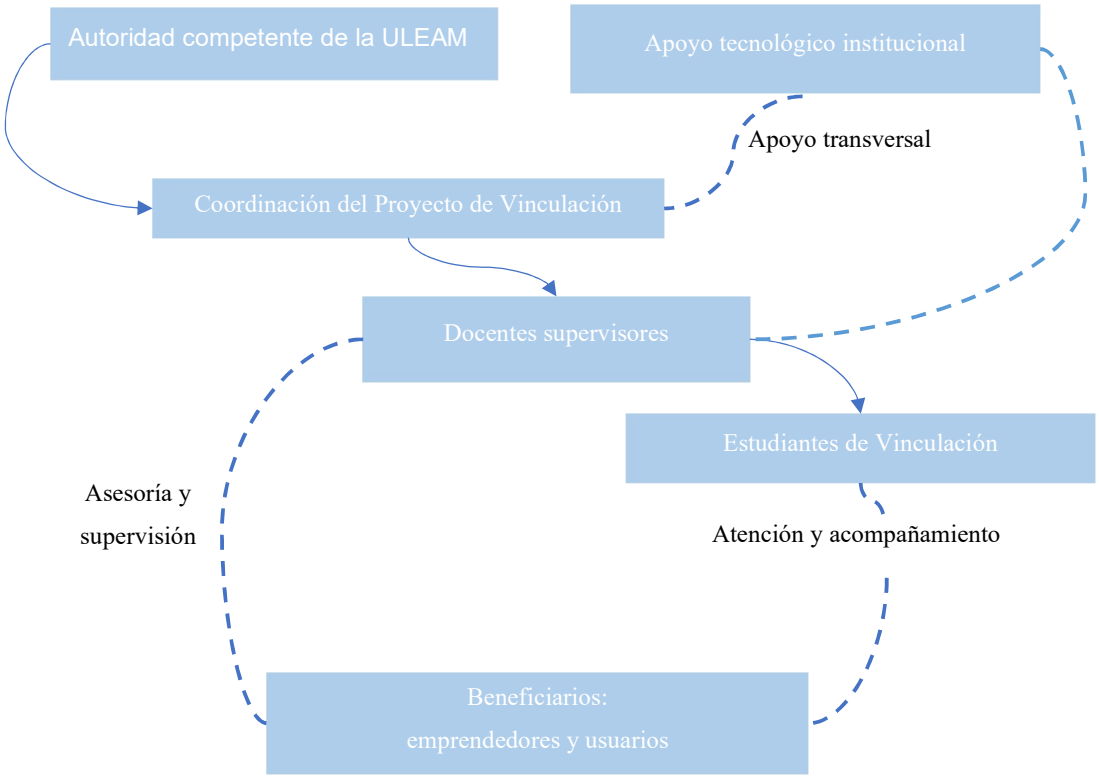
En la auditoría, estos principios tienen una aplicación práctica. La rectitud y la rendición de cuentas ayudan a registrar las actividades realizadas y a conservar los hallazgos obtenidos. Además, la reserva permite que la consulta y el traslado de la información se realicen solo por medios autorizados. Por su parte, la dedicación institucional orienta el cumplimiento y seguimiento de los compromisos establecidos. Asimismo, la innovación permite buscar soluciones tecnológicas que respeten las normas vigentes de la ULEAM. Es importante señalar que estas directrices forman parte del diseño de la propuesta y no representan una ejecución actual. Para aplicarlas en el futuro, será necesario definir funciones claras, elaborar manuales internos, realizar capacitaciones y reunir evidencias que puedan verificarse.

3.6.2.4 Estructura organizativa y responsabilidades

El diagnóstico evidenció que el Centro de Apoyo La U asesora.ec no dispone de una estructura funcional propia formalmente documentada y que existen oportunidades de mejora en la asignación de responsabilidades relacionadas con la información. Un organigrama propuesto indica el nivel de aprobación institucional, coordinación del proyecto, supervisión del profesorado, participación estudiantil y apoyo tecnológico. Esta no es la estructura oficial de la ULEAM, ni introduce nuevos puestos; es una propuesta que necesita aprobación y apoyo institucional antes de su implementación.

Figura 2

Propuesta de organigrama funcional para el Centro de Apoyo La U asesora.ec.



Nota. Elaboración propia. El apoyo tecnológico se plantea como una función transversal dentro del Centro y deberá estar a cargo de una unidad o persona autorizada por la ULEAM. Esta propuesta no implica la creación de una nueva unidad administrativa ni modifica la estructura institucional vigente.

Tabla 9

Responsabilidades propuestas para la aplicación de la guía de seguridad de la información

Actor	Responsabilidad propuesta
Autoridad competente de la ULEAM	Autorizar las acciones que requieran aprobación institucional.
Coordinación del Proyecto de Vinculación	Coordinar la aplicación de los lineamientos y el seguimiento de las acciones establecidas.
Docentes supervisores	Orientar y supervisar el cumplimiento de los lineamientos durante las actividades del Centro.

Estudiantes de vinculación	Aplicar las medidas establecidas para el acceso, manejo y resguardo de la información.
Apoyo tecnológico institucional	Brindar asistencia técnica en cuentas, accesos, configuraciones, respaldos u otras acciones dentro de sus competencias.
Beneficiarios	Cumplir las disposiciones que les sean aplicables durante el uso de los servicios y recursos del Centro.

Nota. Elaboración propia. Las responsabilidades planteadas se limitan a la aplicación de la guía y estarán sujetas a las competencias y autorizaciones institucionales correspondientes.

3.6.3 Lineamientos de seguridad de la información

Los lineamientos establecen pautas para el manejo de la información utilizada en las actividades del Centro. Su aplicación busca orientar a los participantes sobre las responsabilidades básicas relacionadas con el acceso, uso, almacenamiento y resguardo de los datos, considerando las funciones que desempeña cada actor. Estos lineamientos deberán ser revisados y autorizados por la instancia institucional competente antes de su aplicación.

Tabla 10
Lineamientos propuestos para la seguridad de la información

Lineamiento	Aplicación propuesta
Acceso a la información	Permitir el acceso únicamente a las personas autorizadas, de acuerdo con las funciones y actividades asignadas.
Uso de cuentas	Utilizar cuentas individuales cuando estén disponibles y evitar compartir usuarios, contraseñas u otras credenciales de acceso.
Roles y permisos	Asignar permisos según las funciones de cada usuario y revisarlos cuando existan cambios de responsabilidad o participación.
Manejo de información personal	Utilizar los datos personales únicamente para las actividades autorizadas y evitar su reproducción o divulgación innecesaria.
Respaldo de información	Realizar respaldos de la información necesaria para las actividades del Centro y mantener evidencia de su ejecución y verificación.
Reporte de incidentes	Comunicar oportunamente pérdidas de información, accesos no autorizados, fallas u otras situaciones que puedan afectar su seguridad.
Gestión de riesgos	Registrar y valorar los riesgos identificados para establecer acciones, responsables y mecanismos de seguimiento.
Revisión de controles	Revisar periódicamente la aplicación de las medidas establecidas y documentar las acciones de mejora cuando se identifiquen debilidades.

Nota. Elaboración propia a partir de las necesidades identificadas durante el diagnóstico. Su aplicación estará sujeta a las competencias y autorizaciones institucionales correspondientes.

3.6.4 Gestión de cuentas, autenticación, roles y permisos de acceso

La gestión de accesos busca establecer un control ordenado sobre las personas que utilizan los recursos y la información del Centro. Para ello, se plantean medidas relacionadas con la asignación de cuentas, el uso de credenciales, la definición de permisos y la revisión de accesos cuando existan cambios en las funciones o en la participación de los usuarios. Estas acciones deberán ejecutarse únicamente por las personas o unidades que cuenten con la autorización institucional correspondiente.

Tabla 11

Procedimiento propuesto para la gestión de cuentas y accesos

Actividad	***Acción propuesta***	***Responsable***	***Evidencia***
Solicitud de acceso	Identificar la necesidad de acceso y el recurso requerido según la función del usuario.	Coordinación / docente supervisor	Solicitud o registro
Autorización	Verificar y autorizar el acceso antes de su asignación.	Responsable autorizado	Registro de autorización
Asignación de cuenta	Gestionar una cuenta individual cuando el recurso lo permita.	Apoyo tecnológico institucional	Registro de cuenta
Asignación de permisos	Otorgar únicamente los permisos necesarios según las actividades asignadas.	Responsable autorizado / apoyo tecnológico	Matriz de roles y permisos
Uso de credenciales	Mantener las credenciales de forma individual y evitar su intercambio entre usuarios.	Usuario autorizado	Registro o aceptación del lineamiento
Revisión de accesos	Comprobar que los permisos continúen correspondiendo a las funciones del usuario.	Coordinación / apoyo tecnológico	Registro de revisión
Retiro o modificación	Solicitar la modificación o eliminación del acceso cuando cambien las funciones o finalice la participación del usuario.	Coordinación / responsable autorizado	Registro de modificación o baja

Nota. Elaboración propia. La asignación, modificación o eliminación de cuentas y permisos estará sujeta a las competencias y autorizaciones institucionales correspondientes.

El procedimiento establece una secuencia para controlar el acceso desde su solicitud hasta su modificación o retiro. De esta manera, cada acceso queda asociado con una necesidad,

una autorización y una responsabilidad definida, evitando que la asignación de cuentas y permisos se realice de manera informal. Como complemento, se propone una matriz de roles y permisos que permita registrar el nivel de acceso correspondiente a cada participante.

Tabla 12
Matriz propuesta de roles y permisos de acceso

Rol	Recurso o información	Acceso propuesto	Autorización	Revisión
Coordinación del Proyecto	Documentación administrativa y registros del Centro	Lectura, registro y gestión según sus funciones	Autoridad competente	Periódica
Docentes supervisores	Documentación de actividades y registros bajo su supervisión	Lectura y edición según actividad asignada	Coordinación	Al cambiar funciones
Estudiantes de vinculación	Información necesaria para actividades asignadas	Acceso limitado a la actividad	Docente supervisor / Coordinación	Al inicio y fin de participación
Apoyo tecnológico institucional	Recursos tecnológicos que requieran soporte	Acceso técnico autorizado	Instancia competente	Según necesidad
Beneficiarios	Información y recursos habilitados para el servicio recibido	Acceso limitado	Responsable de la actividad	Durante la atención

Nota. Elaboración propia. Los niveles de acceso son referenciales y deberán ajustarse a los recursos disponibles, las funciones asignadas y las autorizaciones institucionales correspondientes.

La matriz permite delimitar el acceso de cada participante según las funciones que desempeña y los recursos que necesita para realizar sus actividades. Los permisos deberán revisarse cuando exista un cambio de funciones, finalice la participación de un usuario o se modifiquen los recursos utilizados, manteniendo el registro de la autorización correspondiente.

3.6.5 Respaldo y recuperación de la información

El respaldo y la recuperación requieren una organización previa que permita determinar qué información debe conservarse, con qué frecuencia se realizará la copia y quién será responsable de verificarla. Para ello, se propone un procedimiento que permita registrar estas actividades y comprobar que la información pueda recuperarse cuando sea necesario.

Tabla 13

Procedimiento propuesto para el respaldo y recuperación de la información

Actividad	Acción propuesta	Responsable	Evidencia
Identificación	Determinar la información que requiere respaldo según su importancia para las actividades del Centro.	Coordinación / docente supervisor	Registro de información a respaldar
Programación	Establecer la frecuencia del respaldo de acuerdo con el uso y actualización de la información.	Coordinación / apoyo tecnológico	Cronograma de respaldos
Ejecución	Realizar la copia en el medio o repositorio institucional autorizado.	Responsable autorizado	Bitácora de respaldo
Verificación	Comprobar que la copia se haya generado correctamente y pueda ser localizada.	Responsable autorizado	Registro de verificación
Prueba de recuperación	Realizar una recuperación controlada para comprobar que la información respaldada pueda restaurarse.	Apoyo tecnológico institucional	Registro de prueba
Atención de pérdida	Recuperar la versión disponible cuando ocurra una pérdida o incidente, previa autorización correspondiente.	Responsable autorizado / apoyo tecnológico	Registro de recuperación
Seguimiento	Registrar fallas detectadas y las acciones tomadas para corregirlas.	Coordinación	Registro de acciones de mejora

Nota. Elaboración propia. Los medios de almacenamiento, periodicidad y responsables deberán ajustarse a los recursos disponibles y a las disposiciones institucionales de la ULEAM.

El procedimiento permite mantener evidencia de cada respaldo y comprobar su disponibilidad mediante verificaciones y pruebas de recuperación. La frecuencia y el medio

utilizado no se establecen de forma fija en la guía, debido a que deberán definirse según la importancia de la información, los recursos disponibles y las disposiciones institucionales aplicables.

Tabla 14

Registro propuesto de respaldo y recuperación de la información

Fecha	Información respaldada	Tipo de actividad	Medio o ubicación autorizada	Responsable	Resultado	Observación
		Respaldo / Recuperación / Prueba			Satisfactorio / Con novedad	

Nota. Elaboración propia. El registro deberá completarse cada vez que se realice un respaldo, recuperación o prueba, utilizando únicamente medios o ubicaciones autorizadas por la institución.

La información consignada en este formato permitirá verificar cuándo se efectuó cada actividad, quién estuvo a cargo y cuál fue su resultado. Las novedades detectadas deberán quedar registradas para que puedan ser atendidas y consideradas en las revisiones posteriores.

3.6.6 Gestión de riesgos de seguridad de la información

La gestión de riesgos se incorpora en la guía para organizar la identificación y valoración de situaciones que puedan afectar la información utilizada en el Centro. Para cada riesgo se considerará su probabilidad de ocurrencia y el impacto que podría generar, lo que permitirá determinar su nivel de prioridad y definir las acciones necesarias para su tratamiento. Los resultados deberán registrarse junto con el responsable y las medidas previstas para su revisión posterior.

Tabla 15

Criterios propuestos para valorar el impacto de los riesgos

Impacto	Descripción	Aspectos que deben considerarse
Alto	La consecuencia puede afectar de forma importante la confidencialidad, integridad o disponibilidad de información relevante, especialmente cuando involucra	Sensibilidad de la información, cantidad de personas o actividades afectadas, duración de la interrupción

Impacto	Descripción	Aspectos que deben considerarse
	datos personales o actividades necesarias para el funcionamiento del Centro.	y posibles consecuencias para el Centro.
Medio	La consecuencia puede afectar parcialmente la información o las actividades del Centro, pero su atención puede realizarse sin comprometer de manera prolongada su funcionamiento.	Alcance de la afectación, tiempo necesario para recuperar la información o actividad y recursos requeridos para atenderla.
Bajo	La consecuencia genera una afectación limitada y puede ser atendida mediante las actividades habituales del Centro, sin producir una interrupción significativa.	Número reducido de personas o recursos afectados, corta duración y facilidad de recuperación.

Nota. Elaboración propia. La valoración del impacto se realizará considerando la afectación que el riesgo podría generar sobre la confidencialidad, integridad o disponibilidad de la información y sobre las actividades del Centro.

Tabla 16

Criterios propuestos para valorar la probabilidad de los riesgos

Nivel	Descripción	Aspectos que deben considerarse
Alta	Existen condiciones que hacen probable que el riesgo ocurra o vuelva a presentarse durante las actividades del Centro.	Antecedentes de ocurrencia, debilidades existentes, frecuencia de la actividad y ausencia o insuficiencia de medidas de control.
Media	El riesgo podría presentarse bajo determinadas condiciones, aunque existen medidas que reducen parcialmente su posibilidad de ocurrencia.	Controles existentes, frecuencia de exposición y situaciones que podrían favorecer su ocurrencia.
Baja	La ocurrencia del riesgo es poco frecuente debido a las condiciones existentes o a la aplicación de medidas que reducen su posibilidad.	Controles aplicados, antecedentes disponibles y baja exposición a la situación evaluada.

Nota. Elaboración propia. La probabilidad se valorará considerando las condiciones existentes, los antecedentes disponibles y las medidas aplicadas para reducir la posibilidad de ocurrencia del riesgo.

Tabla 17

Criterios propuestos para determinar el nivel de riesgo

Impacto / Probabilidad	Baja	Media	Alta
Alto (3)	Medio (3)	Alto (6)	Alto (9)
Medio (2)	Bajo (2)	Medio (4)	Alto (6)
Bajo (1)	Bajo (1)	Bajo (2)	Medio (3)

Nota. Los valores se utilizan para relacionar el impacto y la probabilidad y establecer el nivel de riesgo como bajo, medio o alto. La matriz se emplea como herramienta de apoyo para priorizar los riesgos identificados y orientar su tratamiento. Elaboración propia con base en las directrices de ISO/IEC 27005:2022 (ISO, 2022a).

El resultado obtenido permite ordenar los riesgos según su nivel y reconocer cuáles requieren mayor atención. La valoración sirve como referencia para definir el tratamiento correspondiente, considerando las condiciones del Centro, los recursos disponibles y las responsabilidades asignadas.

Tabla 18

Matriz propuesta para el registro y tratamiento de riesgos

Código	Riesgo identificado	Impacto	Probabilidad	Nivel de riesgo	Tratamiento propuesto	Responsable	Plazo	Estado
R-01	[Por completar]	Alto / Medio / Bajo	Alta / Media / Baja	Alto / Medio / Bajo	[Por completar]	[Por completar]	[Por completar]	Pendiente
R-02	[Por completar]							
R-03	[Por completar]							

Nota. laboración propia. La matriz se completará cuando se aplique la guía. El nivel de riesgo se determinará mediante los criterios establecidos en las Tablas 15, 16 y 17. El tratamiento, responsable y plazo deberán definirse de acuerdo con las condiciones del riesgo y las competencias institucionales correspondientes.

La matriz permitirá mantener organizados los riesgos identificados y las decisiones adoptadas para su atención. Su actualización deberá realizarse cuando cambien las condiciones evaluadas, se ejecuten las acciones previstas o se identifiquen nuevas situaciones que puedan afectar la seguridad de la información.

3.6.7 Revisión y seguimiento de los controles

La revisión de los controles permitirá conocer si las medidas establecidas en la guía se están aplicando y si requieren ajustes durante su utilización. Para ello, se propone registrar el control revisado, el resultado obtenido, las acciones necesarias y la persona responsable de atenderlas. La periodicidad de estas revisiones deberá definirse de acuerdo con las actividades del Centro y las disposiciones institucionales correspondientes.

Tabla 29
Registro propuesto para la revisión y seguimiento de controles

Control o medida revisada	Resultado de la revisión	Acción requerida	Responsable	Fecha de compromiso	Estado	Evidencia de cumplimiento
[Por completar]	[Por completar]	[Por completar]	[Por completar]	[Por completar]	Pendiente / En ejecución / Completada	[Por completar]

Nota. Elaboración propia. Los campos se completarán durante la aplicación de la guía. El estado permitirá identificar el avance de cada acción y la evidencia de cumplimiento deberá corresponder con la actividad realizada.

Los resultados de las revisiones servirán para identificar medidas que requieren ajustes o acciones adicionales. Cuando una actividad no se haya completado, deberá mantenerse pendiente hasta contar con el respaldo correspondiente y la verificación de su cumplimiento por la persona responsable.

3.6.8 Formatos de apoyo de la guía

Para apoyar la aplicación de los lineamientos y procedimientos establecidos, la guía incorpora formatos destinados al registro de actividades relacionadas con accesos, respaldos, riesgos y seguimiento de controles. Estos instrumentos permiten organizar la información generada durante su aplicación y conservar un registro de las acciones realizadas, sin modificar las competencias establecidas por la institución.

Tabla 20
Formatos de apoyo incorporados en la guía

Formato	Finalidad
Matriz de roles y permisos de acceso	Registrar los niveles de acceso asignados de acuerdo con las funciones de cada participante.

Registro de respaldo y recuperación	Documentar las actividades de respaldo, recuperación y pruebas realizadas.
Matriz de registro y tratamiento de riesgos	Organizar los riesgos identificados, su valoración y las acciones previstas para su tratamiento.
Registro de revisión y seguimiento de controles	Documentar los resultados de las revisiones, acciones requeridas, responsables y estado de cumplimiento.

Nota. Elaboración propia. Los formatos forman parte de la propuesta y deberán completarse durante la aplicación de la guía, de acuerdo con las autorizaciones y responsabilidades institucionales correspondientes.

Los formatos complementan los procedimientos planteados y permiten mantener organizada la información generada durante la aplicación de la guía. Su utilización podrá ajustarse a las condiciones operativas del Centro, siempre que se conserven los campos necesarios para identificar responsables, actividades realizadas y resultados obtenidos.

CONCLUSIONES

La evolución del uso de recursos digitales ha incrementado la necesidad de proteger la información frente a situaciones que puedan comprometer su confidencialidad, integridad y disponibilidad. En este contexto, la auditoría informática constituye un mecanismo de evaluación que ayuda a reconocer el estado de los controles y las condiciones que pueden generar exposición al riesgo.

El análisis teórico evidenció una relación directa entre la auditoría informática y la salvaguarda de los datos, debido a que la evaluación sistemática de los controles permite contrastar las prácticas existentes con criterios previamente establecidos. Los fundamentos estudiados proporcionaron el sustento conceptual, técnico y normativo necesario para orientar el estudio y establecer los aspectos considerados durante la revisión.

La situación actual del Centro de Apoyo La U Asesor@.ec presenta principalmente necesidades de formalización y organización en el manejo de la información. La revisión realizada mostró prácticas que requieren mayor control en el uso de cuentas, asignación de permisos, respaldos, gestión de riesgos y monitoreo, además de documentación insuficiente para demostrar de manera consistente cómo se ejecutan y supervisan estas actividades.

partir de las necesidades detectadas se estructuró una guía que integra lineamientos, responsabilidades, procedimientos y registros para ordenar las prácticas relacionadas con accesos, respaldos, riesgos y seguimiento. La propuesta proporciona al Centro una herramienta documental adaptable a sus condiciones de funcionamiento, cuya aplicación queda sujeta a la revisión y autorización de las instancias institucionales competentes.

.

.

RECOMENDACIONES

Promover revisiones periódicas de los recursos y prácticas tecnológicas utilizadas en el Centro, de manera que la auditoría informática contribuya a reconocer oportunamente riesgos, cambios y necesidades de mejora. Estas revisiones permitirán mantener una visión actualizada de las condiciones en las que se maneja la información y orientar las acciones que requieran atención.

A partir de estas revisiones, fortalecer la evaluación de los controles de TI mediante criterios técnicos y normativos aplicables a las actividades del Centro. Esto permitirá valorar no solo el funcionamiento de los recursos tecnológicos, sino también la forma en que los controles contribuyen a preservar la confidencialidad, integridad y disponibilidad de la información.

Como parte de este fortalecimiento, establecer mecanismos de control y documentación que aporten trazabilidad a las actividades realizadas. La definición de responsables y el mantenimiento de registros facilitarán la verificación de las acciones ejecutadas, el seguimiento de situaciones pendientes y la disponibilidad de información para futuras revisiones y toma de decisiones.

Finalmente, presentar la guía de seguridad de la información ante las instancias competentes de la ULEAM para valorar su aplicación en el Centro de Apoyo La U Asesor@.ec. De ser autorizada, su utilización progresiva permitirá integrar los controles de TI, la gestión de riesgos y el seguimiento de las acciones de mejora dentro de una herramienta ajustable a las necesidades del Centro.

Referencias

AlGhamdi, S., Win, K. T., & Vlahu-Gjorgievska, E. (2020). Information security governance challenges and critical success factors: Systematic review. Computers & Security, 99, 102030. https://doi.org/10.1016/j.cose.2020.102030

Antunes, M., Maximiano, M., & Gomes, R. (2022). A customizable web platform to manage standards compliance of information security and cybersecurity auditing. Procedia Computer Science, 196, 36–43. https://doi.org/10.1016/j.procs.2021.11.070

Asamblea Nacional del Ecuador. (2021). Ley Orgánica de Protección de Datos Personales. Quinto Suplemento del Registro Oficial No. 459. https://www.asambleanacional.gob.ec/es/multimedios-legislativos/63464-ley-organica-de-proteccion-de-datos

Burgos-Rojas, M. A., Haro-Polo, C. I., & Mendoza-de los Santos, A. C. (2024). Impacto del uso de diversos marcos de seguridad en las auditorías informáticas dentro de las organizaciones: Revisión sistemática. Revista Científica de la UCSA, 11(2), 103–115. https://doi.org/10.18004/ucsa/2409-8752/2024.011.02.0103

Cheng, E. C. K., & Wang, T. (2022). Institutional strategies for cybersecurity in higher education institutions. Information, 13(4), 192. https://doi.org/10.3390/info13040192

Chidukwani, A., Zander, S., & Koutsakis, P. (2022). A survey on the cyber security of small-to-medium businesses: Challenges, research focus and recommendations. IEEE Access, 10, 85701–85719. https://doi.org/10.1109/ACCESS.2022.3197899

Constitución de la República del Ecuador. (2008). Registro Oficial No. 449.

Creswell, J. W., & Creswell, J. D. (2022). Research design: Qualitative, quantitative, and mixed methods approaches (6th ed.). SAGE Publications.

Garcés Córdova, F. A., Díaz Basurto, I. J., & Moreno Arvelo, P. M. (2023). Evaluación del derecho al olvido en la salvaguarda de datos personales en Ecuador. Dilemas Contemporáneos: Educación, Política y Valores, 11(Edición especial), Artículo 80. https://doi.org/10.46377/dilemas.v11iEspecial.3949

International Organization for Standardization. (2022a). Information security, cybersecurity and privacy protection—Guidance on managing information security risks (ISO/IEC 27005:2022). https://www.iso.org/standard/80585.html

International Organization for Standardization. (2022b). Information security, cybersecurity and privacy protection—Information security controls (ISO/IEC 27002:2022). https://www.iso.org/standard/75652.html

International Organization for Standardization. (2022c). Information security, cybersecurity and privacy protection—Information security management systems—Requirements (ISO/IEC 27001:2022). https://www.iso.org/standard/27001

International Organization for Standardization. (2026). Guidelines for auditing management systems (ISO 19011:2026). https://www.iso.org/standard/19011

Joint Task Force. (2020). Security and privacy controls for information systems and organizations (NIST Special Publication 800-53, Revision 5). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-53r5

Littan, S. H., Herz, R. H., Hirth, R. B., Jr., Hileman, D., Monterio, B. J., & Thomson, J. C. (2023). Achieving effective internal control over sustainability reporting (ICSR): Building trust and confidence through the COSO Internal Control—Integrated Framework. Committee of Sponsoring Organizations of the Treadway Commission. https://www.coso.org/_files/ugd/3059fc_5949d4d5f3f74e2ea9ee11ce4b68b603.pdf

Lucero, L. (2023). El rol de la auditoría informática en la era de la protección de datos personales en Ecuador. Technology Rain Journal, 2(2), e17. https://doi.org/10.55204/trj.v2i2.e17

Ministerio de Telecomunicaciones y de la Sociedad de la Información. (2022). Estrategia Nacional de Ciberseguridad del Ecuador. Gobierno del Ecuador. https://aportecivico.gobiernoelectronico.gob.ec/system/documents/attachments/000/000/103/original/04bfdeb041e78cdc522f3d095f340a5dea2f0083.pdf

National Institute of Standards and Technology. (2020). NIST Privacy Framework: A tool for improving privacy through enterprise risk management, version 1.0 (NIST Cybersecurity White Paper 10). https://doi.org/10.6028/NIST.CSWP.10

National Institute of Standards and Technology. (2024). The NIST Cybersecurity Framework (CSF) 2.0 (NIST Cybersecurity White Paper 29). https://doi.org/10.6028/NIST.CSWP.29

Pawar, S., & Palivela, H. (2022). LCCI: A framework for least cybersecurity controls to be implemented for small and medium enterprises (SMEs). International Journal of Information Management Data Insights, 2(1), 100080. https://doi.org/10.1016/j.jjimei.2022.100080

Presidencia de la República del Ecuador. (2023). Reglamento General de la Ley Orgánica de Protección de Datos Personales (Decreto Ejecutivo No. 904). Tercer Suplemento del Registro Oficial No. 435. https://www.telecomunicaciones.gob.ec/wp-content/uploads/2023/11/Decreto-Ejecutivo-No.-904.pdf

Prümmer, J., van Steen, T., & van den Berg, B. (2024). A systematic review of current cybersecurity training methods. Computers & Security, 136, 103585. https://doi.org/10.1016/j.cose.2023.103585

Rafeq, A., & Elangovan, N. (2021, May 26). A systematic approach to implementing a governance system using COBIT 2019: A COVID-19 case study. ISACA. https://www.isaca.org/resources/news-and-trends/industry-news/2021/a-systematic-approach-to-implementing-a-governance-system-using-cobit-2019

Sabillon, R., Higuera, J. R. B., Cano, J., Higuera, J. B., & Montalvo, J. A. S. (2024). Assessing the effectiveness of cyber domain controls when conducting cybersecurity audits: Insights from higher education institutions in Canada. Electronics, 13(16), 3257. https://doi.org/10.3390/electronics13163257

Sánchez-García, I. D., San Feliu Gilabert, T., & Calvo-Manzano, J. A. (2023). Countermeasures and their taxonomies for risk treatment in cybersecurity: A systematic mapping review. Computers & Security, 128, 103170. https://doi.org/10.1016/j.cose.2023.103170

Saunders, M., Lewis, P., & Thornhill, A. (2023). Research methods for business students (9th ed.). Pearson.

Schmitz, C., Schmid, S., Harborth, D., & Pape, S. (2021). Maturity level assessments of information security controls: An empirical analysis of practitioners' assessment capabilities. Computers & Security, 108, 102306. https://doi.org/10.1016/j.cose.2021.102306

Shillair, R., Esteve-González, P., Dutton, W. H., Creese, S., Nagyfejeo, E., & von Solms, B. (2022). Cybersecurity education, awareness raising, and training initiatives: National level evidence-based results, challenges, and promise. Computers & Security, 119, 102756. https://doi.org/10.1016/j.cose.2022.102756

Slapničar, S., Vuko, T., Čular, M., & Drašček, M. (2022). Effectiveness of cybersecurity audit. International Journal of Accounting Information Systems, 44, 100548. https://doi.org/10.1016/j.accinf.2021.100548

Taherdoost, H. (2022). Understanding cybersecurity frameworks and information security standards—A review and comprehensive overview. Electronics, 11(14), 2181. https://doi.org/10.3390/electronics11142181

Temoshok, D., Fenton, J. L., Choong, Y.-Y., Lefkovitz, N., Regenscheid, A., Galluzzo, R., & Richer, J. P. (2025). Digital identity guidelines: Authentication and authenticator management (NIST Special Publication 800-63B-4). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-63B-4

Ulven, J. B., & Wangen, G. (2021). A systematic review of cybersecurity risks in higher education. Future Internet, 13(2), 39. https://doi.org/10.3390/fi13020039

Universidad Laica Eloy Alfaro de Manabí, Extensión El Carmen. (2025). Proyecto de Vinculación y Emprendimiento: Centro de Apoyo y Asesoría Gratuita en la Gestión Empresarial y de Emprendimiento “La U Asesor@.ec”.

Whitman, M. E., & Mattord, H. J. (2022). Principles of information security (7th ed.). Cengage.

ANEXOS

INSTRUMENTO N.º 3

CHECKLIST DE AUDITORÍA INFORMÁTICA

Basado en ISO/IEC 27001:2022

Objetivo: Verificar el cumplimiento de controles relacionados con la seguridad de la información.

Escala

- Cumple (C)
- Cumple parcialmente (CP)
- No cumple (NC)
- No aplica (NA)

N.º		C	CP	NC	NA	Evidencia/Observación
1	Existe política de seguridad informática documentada			X		No se encontró ningún manual, reglamento o documento oficial aprobado que establezca las políticas de seguridad de la información en la institución.
2	Existe inventario actualizado de equipos informáticos		X			Se encontró un registro básico, pero **no se halló evidencia** de que esté actualizado con las últimas adquisiciones ni con las especificaciones técnicas completas (ej. RAM, discos, direcciones IP).
3	Existe inventario de activos de información		X			Se evidenció un listado parcial, pero **ausencia de un registro integral** que clasifique el nivel de criticidad de todas las bases de datos y archivos físicos/digitales.
4	Cada usuario posee una cuenta individual			X		No se encontró un sistema de autenticación individualizada; mediante inspección se comprobó el uso de cuentas de acceso genéricas en varios equipos.
5	No existen cuentas compartidas			X		Se evidenció la carencia de controles de inicio de sesión; se constató que múltiples empleados

N.º		C	CP	NC	NA	Evidencia/Observación
						del área administrativa ingresan a los sistemas con el mismo usuario y contraseña.
6	Las contraseñas cumplen criterios mínimos de seguridad		X			El sistema exige clave, pero **no se encontraron configuraciones (políticas de Active Directory)** que fuercen la longitud mínima, ni el uso de caracteres especiales o alfanuméricos.
7	Se cambian periódicamente las contraseñas			X		No se evidenció ninguna política en el sistema que obligue al usuario a renovar su contraseña tras un periodo determinado (caducidad de clave inactiva).
8	Los permisos de acceso se asignan según las funciones del usuario			X		Ausencia de matrices de roles y perfiles; no se encontró segregación de funciones, otorgando privilegios de administrador a usuarios operativos.
9	Se eliminan oportunamente los accesos de usuarios que dejan la institución			X		Al revisar los sistemas, **no se halló un procedimiento de desvinculación**; se encontraron cuentas activas de personal que ya no labora en la institución.
10	Existe control sobre el acceso a carpetas compartidas			X		No se evidenció restricción de permisos en red; las carpetas compartidas son de acceso público para cualquier equipo conectado a la red local (LAN).
11	Los documentos confidenciales poseen acceso restringido		X			Aunque existen algunos archivos con contraseña, **no se encontró una política estandarizada de cifrado** ni protección sistemática para la información financiera o sensible.
12	Se controla el uso de memorias USB			X		No se halló ningún software de control de terminales (Endpoint Security) ni directivas de grupo que restrinjan o auditen la lectura/escritura en puertos USB.
13	Existe antivirus instalado y actualizado	X				Se evidenció mediante revisión en pantalla que los equipos cuentan con software antivirus con licencias vigentes y firmas de virus actualizadas a la fecha.
14	El sistema operativo se mantiene actualizado	X				Se constató en la configuración de los equipos (Windows Update) que las actualizaciones de seguridad están activas y descargando los últimos parches.

N.º		C	CP	NC	NA	Evidencia/Observación
15	Existe firewall activo en los equipos			X		No se encontró un firewall perimetral de red, y mediante revisión en los equipos de trabajo, el Firewall local del sistema operativo se encontraba desactivado.
16	Los equipos cuentan con bloqueo automático de pantalla		X			Se observó en algunos equipos, pero **no se encontró una política de grupo (GPO)** configurada desde el servidor que automatice este bloqueo en toda la red tras inactividad.
17	Se realizan copias de seguridad periódicas			X		No se encontró cronograma, bitácora ni software automatizado que evidencie la ejecución de respaldos (backups) diarios o semanales.
18	Los respaldos son almacenados en un lugar seguro			X		Al no haber respaldos, **tampoco se halló un servidor alterno, almacenamiento en la nube, ni bóveda física** externa segura para salvaguardar la información.
19	Se verifica periódicamente la recuperación de respaldos			X		Ausencia de actas, informes o registros que demuestren que se hayan realizado pruebas de restauración (recovery tests) de los datos.
20	Existe un procedimiento para recuperación ante pérdida de información			X		No se encontró ningún Plan de Recuperación ante Desastres (DRP) ni manual de contingencia documentado para restaurar la operatividad en caso de incidentes.
21	La información se almacena en plataformas autorizadas			X		No se hallaron repositorios institucionales oficiales; se evidenció que los usuarios utilizan plataformas personales no controladas (Google Drive/Dropbox personal) para guardar datos institucionales.
22	Se evita almacenar información institucional en dispositivos personales			X		No se encontró evidencia de controles que lo impidan; por el contrario, se constató el uso de laptops y pendrives personales procesando información de la entidad.
23	Existe control sobre documentos impresos con información confidencial		X			Existen archivadores con llave, pero **no se encontró aplicación de la política de "Escritorios Limpios"**; se dejaron documentos sensibles sobre los escritorios fuera del horario laboral.

N.º		C	CP	NC	NA	Evidencia/Observación
24	Los equipos permanecen en áreas seguras	X				Se evidenció visualmente que los servidores y equipos principales de red están ubicados en un rack cerrado dentro de un área física delimitada.
25	Existe control de ingreso a las áreas donde se almacena información	X				Se constató que el área de servidores y archivo físico cuenta con cerraduras y el acceso está restringido exclusivamente al personal designado.
26	Se reportan incidentes de seguridad informática			X		No se encontró ningún formato, sistema de tickets (Mesa de Ayuda) ni canal de comunicación formal establecido para que los usuarios reporten anomalías informáticas.
27	Existe un registro de incidentes			X		Ausencia total de bitácoras, matrices o bases de datos que documenten el historial de fallos, ataques por malware o pérdidas de información.
28	Se aplican acciones correctivas después de un incidente			X		Al no existir registros de incidentes, **tampoco se hallaron planes de acción**, informes de resolución, ni análisis de causa raíz.
29	El personal recibe capacitación en seguridad informática			X		En los archivos de Talento Humano **no se encontró evidencia (certificados, actas de asistencia)** de planes de capacitación en concientización sobre ciberseguridad.
30	Existe conocimiento sobre la Ley Orgánica de Protección de Datos Personales			X		Mediante sondeos verbales, se evidenció **desconocimiento total** por parte del personal administrativo sobre las obligaciones y sanciones de la normativa de protección de datos vigente.
31	Se informa a los usuarios sobre el tratamiento de sus datos personales			X		No se encontraron acuerdos de confidencialidad (NDAs), avisos de privacidad, ni formularios de consentimiento firmados por empleados o clientes para el tratamiento de su información.
32	Los documentos digitales están correctamente organizados		X			Existen carpetas departamentales, pero **no se halló una nomenclatura o taxonomía estandarizada** para nombrar archivos, lo que genera duplicidad y desorden.
33	Los archivos poseen una estructura de almacenamiento definida			X		No se encontró un árbol de directorios institucional estructurado ni un manual de archivo digital que estandarice el almacenamiento.

N.º		C	CP	NC	NA	Evidencia/Observación
34	Existe control sobre la eliminación de documentos			X		No se encontraron restricciones de borrado; cualquier usuario con acceso a las carpetas en red posee los permisos necesarios para eliminar archivos definitivos sin dejar rastro de auditoría.
35	Se protege la información compartida mediante correo electrónico			X		No se evidenció el uso de cifrado, contraseñas en adjuntos, ni firmas digitales institucionales al transmitir información confidencial (ej. nóminas, balances) vía email.
36	Los equipos utilizados para la atención al público están protegidos		X			Existen pantallas en el área de atención, pero **no se hallaron filtros de privacidad** físicos en los monitores, permitiendo a terceros visualizar parcialmente información confidencial desde el mostrador.
37	Existe revisión periódica de los controles informáticos			X		No se encontró ningún comité de seguridad de la información, ni designación de responsables que validen y monitoreen la eficacia de los controles establecidos.
38	Se evalúan los riesgos relacionados con la información			X		Ausencia de una Matriz de Riesgos Informáticos; no se evidenció ningún análisis documentado que identifique amenazas, vulnerabilidades o impacto potencial sobre los activos.
39	Existe seguimiento al cumplimiento de los controles implementados			X		No se encontraron informes de gestión, actas de revisión por la dirección, ni indicadores de desempeño (KPIs) orientados a medir el nivel de seguridad informática.
40	La institución realiza auditorías o evaluaciones periódicas de seguridad informática			X		No se encontraron dictámenes, informes finales, ni planes de auditoría informática (interna o externa) ejecutados en ejercicios o periodos fiscales anteriores.

ANEXO B: REPORTE FOTOGRÁFICO DE HALLAZGOS Y EVIDENCIAS

Institución de Educación Superior: Universidad Laica Eloy Alfaro de Manabí, Extensión El Carmen

Carrera: Auditoría y Control de Gestión

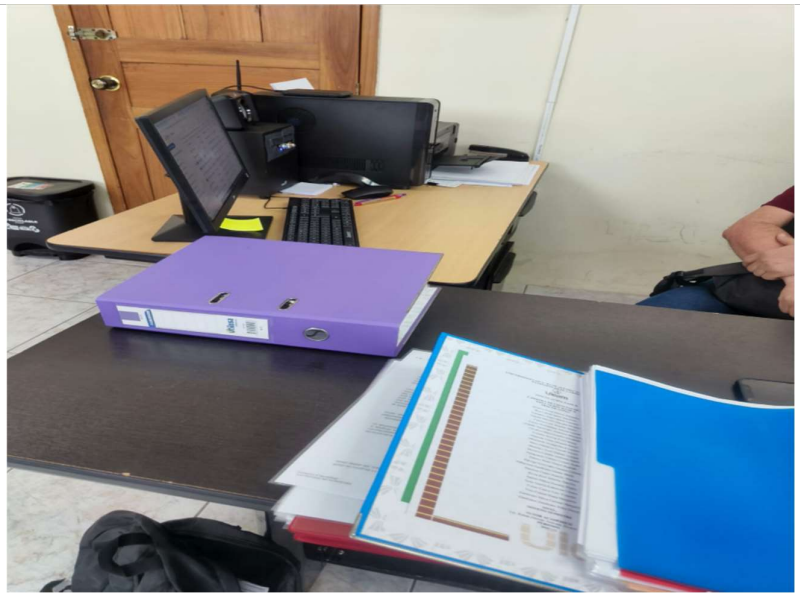
Equipo Auditor:

- Michael Rodrigo Morocho Ribadeneira

Objetivo: Documentar gráficamente los hallazgos identificados durante la evaluación in situ de los controles de seguridad de la información.

Anexo N.º 1	**Ref. Checklist: Ítem 15**
Área/Ubicación:	Departamento Administrativo - Equipo "PC-Contabilidad-02"
Fecha de toma:	15/06/2026
Evidencia Gráfica:	
	
Descripción Técnica (Hallazgo):	Captura de pantalla de la configuración del sistema operativo evidenciando que el Firewall de Windows Network se encuentra en estado "Desactivado", lo que justifica la calificación de "No Cumple".

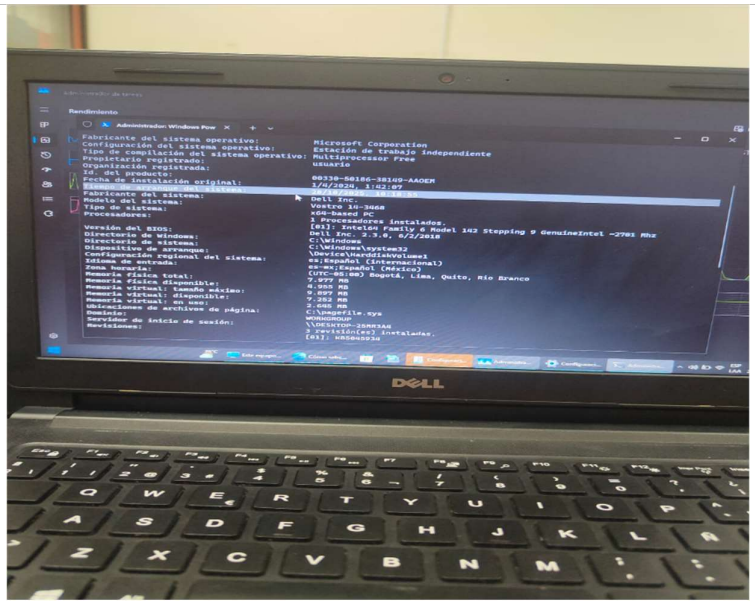
Anexo N.º 2	**Ref. Checklist: Ítem 23**
Área/Ubicación:	Área de Atención al Cliente - Escritorio principal
Fecha de toma:	15/06/2026
Evidencia Gráfica:	

Anexo N.º 2	**Ref. Checklist: Ítem 23**
	
Descripción Técnica (Hallazgo):	Fotografía tomada fuera del horario de atención al público. Se evidencia el incumplimiento de la política de "Escritorios Limpios", encontrándose carpetas con información sensible expuestas sin las debidas seguridades físicas. *(Nota: Datos confidenciales difuminados por seguridad).*

Anexo N.º 3	**Ref. Checklist: Ítem 14**
Área/Ubicación:	Área de Sistemas - Servidor Principal
Fecha de toma:	15/06/2026
Evidencia Gráfica:	

Anexo N.º 3	Ref. Checklist: Ítem 14
	
Descripción Técnica (Hallazgo):	Captura del panel de Windows Update evidenciando que el sistema operativo se encuentra buscando, descargando e instalando los últimos parches de seguridad. Sustenta la calificación de "Cumple".

Anexo N.º 4	Ref. Checklist: Ítem 5
Área/Ubicación:	Departamento Financiero - Equipos operativos
Fecha de toma:	15/06/2026
Evidencia Gráfica:	

Anexo N.º 4	Ref. Checklist: Ítem 5
	
Descripción Técnica (Hallazgo):	Captura de la pantalla de inicio de sesión de Windows evidenciando el uso de una cuenta genérica en lugar de credenciales individuales y personalizadas, lo que sustenta la calificación de "No Cumple".

Anexo N.º 5	Ref. Checklist: Ítem 36
Área/Ubicación:	Recepción / Área de Atención al Público
Fecha de toma:	15/06/2026
Evidencia Gráfica:	

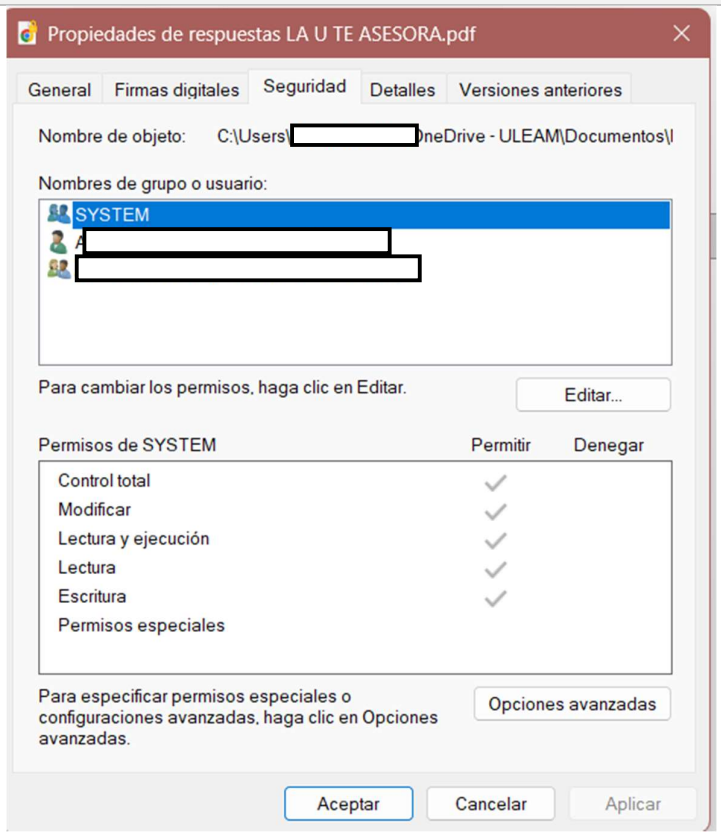
Anexo N.º 5	Ref. Checklist: Ítem 36
	
Descripción Técnica (Hallazgo):	Fotografía tomada desde la perspectiva del usuario externo. Se evidencia que la pantalla del equipo informático es claramente visible para terceros debido a la ausencia de filtros de privacidad físicos, lo que representa un riesgo de exposición de datos (calificación "Cumple Parcialmente").

Anexo N.º 6	Ref. Checklist: Ítem 32
Área/Ubicación:	Red Local Compartida (LAN) - Servidor de Archivos
Fecha de toma:	15/06/2026
Evidencia Gráfica:	
Descripción Técnica (Hallazgo):	Captura de pantalla de la raíz de la carpeta compartida departamental. Se constata la falta de una taxonomía institucional, evidenciando archivos sin nomenclatura

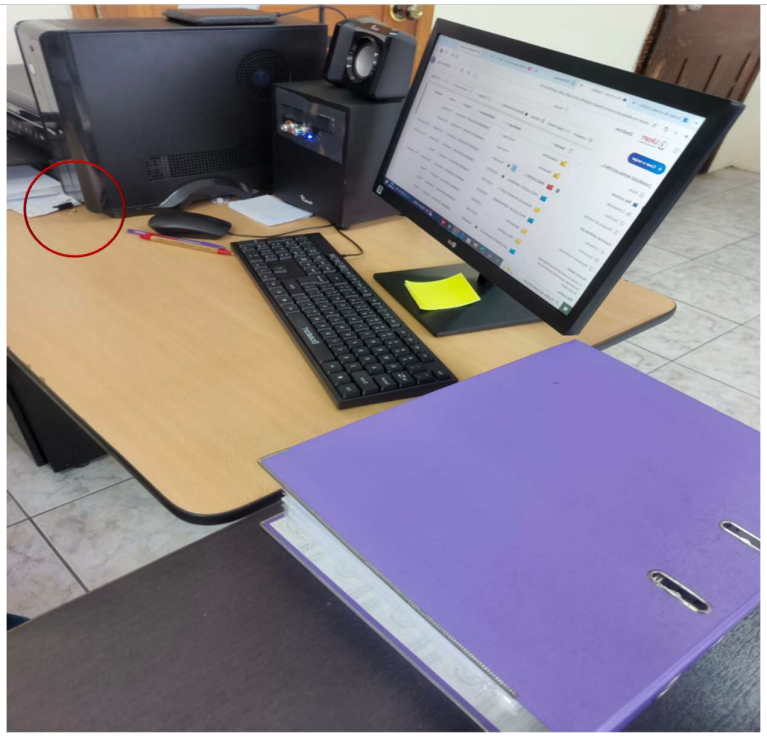
Anexo N.º 6	Ref. Checklist: Ítem 32
	estandarizada y desorden en los niveles de almacenamiento (calificación "Cumple Parcialmente").

Anexo N.º 7	Ref. Checklist: Ítem 25
Área/Ubicación:	Cuarto de Servidores (Data Center) / Archivo Central
Fecha de toma:	15/06/2026
Evidencia Gráfica:	
	
Descripción Técnica (Hallazgo):	Fotografía del acceso al área donde se aloja la infraestructura de red principal. Se evidencia que el perímetro cuenta con seguridad física (puerta con cerradura operativa y letrero de acceso restringido), justificando la calificación de "Cumple".

Anexo N.º 8	Ref. Checklist: Ítem 10 y relacionado al 34
Área/Ubicación:	Entorno de Red - PC Administrativa

Anexo N.º 8	**Ref. Checklist: Ítem 10 y relacionado al 34**
Fecha de toma:	15/06/2026
Evidencia Gráfica:	
	
Descripción Técnica (Hallazgo):	Captura de las propiedades de seguridad de un directorio compartido institucional. Se constata que el grupo de usuarios "Todos" (Everyone) posee permisos de "Control total" y "Modificar", permitiendo la lectura, edición o eliminación no autorizada de la información (calificación "No Cumple").

Anexo N.º 9	**Ref. Checklist: Ítem 22**
Área/Ubicación:	Departamento Administrativo - Puesto de trabajo
Fecha de toma:	15/06/2026
Evidencia Gráfica:	

Anexo N.º 9	Ref. Checklist: Ítem 22
	
Descripción Técnica (Hallazgo):	Inspección visual durante el horario laboral donde se evidencia un dispositivo de almacenamiento masivo personal (memoria USB externa) conectado a un equipo informático institucional procesando información, lo cual infringe los controles de restricción de almacenamiento (calificación "No Cumple").