UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA
FACULTAD DE SISTEMAS Y TELECOMUNICACIONES
INSTITUTO DE POSTGRADO

TÍTULO

Plan de fortalecimiento de la ciberseguridad para los sistemas tributarios del GAD municipal del cantón Salcedo, basado en estándares de seguridad

AUTOR
Villalba Solís, Mónica Paulina

TRABAJO DE TITULACIÓN

Previo a la obtención del grado académico en
MAGÍSTER EN CIBERSEGURIDAD

TUTOR
Oviedo Bayas, Byron Wladimir

Santa Elena, Ecuador
Año 2026

UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA
FACULTAD DE SISTEMAS Y TELECOMUNICACIONES
INSTITUTO DE POSTGRADO

TRIBUNAL DE SUSTENTACIÓN

Validar únicamente en FirmaEC.
Firmado electrónicamente por:
ALICIA GERMANIA ANDRADE VERA

Ing. Alicia Andrade Vera, Mgtr.
COORDINADORA DEL PROGRAMA

Validar únicamente en FirmaEC.
Firmado electrónicamente por:
BYRON WLADIMIR OVIEDO BAYAS

Ing. Byron Oviedo Bayas, Ph.D.
TUTOR

Validar únicamente en FirmaEC.
Firmado electrónicamente por:
JAIME BENJAMIN OROZCO IGUASNIA

Ing. Jaime Orozco Iguasnia, Mgtr.
DOCENTE ESPECIALISTA

Validar únicamente en FirmaEC.
Firmado electrónicamente por:
HENRY OMAR CRUZ CARRILLO

Ing. Henry Cruz Carrillo, Ph.D.
DOCENTE ESPECIALISTA

Validar únicamente en FirmaEC.
Firmado electrónicamente por:
MARIA MARGARITA RIVERA GONZALEZ

Abg. María Rivera González, Mgtr.
SECRETARIA GENERAL
UPSE

UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA
FACULTAD DE SISTEMAS Y TELECOMUNICACIONES
INSTITUTO DE POSTGRADO

CERTIFICACIÓN

Certifico que luego de haber dirigido científica y técnicamente el desarrollo y estructura final del trabajo, este cumple y se ajusta a los estándares académicos, razón por el cual apruebo en todas sus partes el presente trabajo de titulación que fue realizado en su totalidad por **VILLALBA SOLÍS MÓNICA PAULINA**, como requerimiento para la obtención del título de Magíster en Ciberseguridad.

TUTOR

Validar únicamente en FirmaEC.
Firmado electrónicamente por:
BYRON WLADIMIR
OVIEDO BAYAS

Ing. Byron Wladimir Oviedo Bayas, Ph.D.

Santa Elena, 26 de junio de 2026

UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA
FACULTAD DE SISTEMAS Y TELECOMUNICACIONES
INSTITUTO DE POSTGRADO

DECLARACIÓN DE RESPONSABILIDAD

Yo, **VILLALBA SOLÍS MÓNICA PAULINA**

DECLARO QUE:

El trabajo de Titulación, **PLAN DE FORTALECIMIENTO DE LA CIBERSEGURIDAD PARA LOS SISTEMAS TRIBUTARIOS DEL GAD MUNICIPAL DEL CANTÓN SALCEDO, BASADO EN ESTÁNDARES DE SEGURIDAD**, previo a la obtención del título en Magíster en Ciberseguridad, ha sido desarrollado respetando derechos intelectuales de terceros conforme las citas que constan en el documento, cuyas fuentes se incorporan en las referencias o bibliografías. Consecuentemente este trabajo es de mi total autoría.

En virtud de esta declaración, me responsabilizo del contenido, veracidad y alcance del Trabajo de Titulación referido.

Santa Elena, 26 de junio de 2026

EL AUTOR

Validar únicamente en FirmaEC.
Firmado electrónicamente por:
MONICA PAULINA
VILLALBA SOLIS

Villalba Solís Mónica Paulina

UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA

FACULTAD DE SISTEMAS Y TELECOMUNICACIONES
INSTITUTO DE POSTGRADO

CERTIFICACIÓN DE ANTIPLAGIO

Certifico que después de revisar el documento final del trabajo de titulación denominado **PLAN DE FORTALECIMIENTO DE LA CIBERSEGURIDAD PARA LOS SISTEMAS TRIBUTARIOS DEL GAD MUNICIPAL DEL CANTÓN SALCEDO, BASADO EN ESTÁNDARES DE SEGURIDAD**, presentado por la estudiante, **VILLALBA SOLÍS MÓNICA PAULINA** fue enviado al Sistema Antiplagio COMPILATIO, presentando un porcentaje de similitud correspondiente al 7%, por lo que se aprueba el trabajo para que continúe con el proceso de titulación.


Certificado de análisis
Compilatio Magister+ | UPSE-ECU

Paulina_Villalba_Proyecto_tesis_8
ID : 3fee71155e864294ab19f5a246468d2c9cd04f6e

7%
Textos sospechosos

Nombre del fichero : Paulina_Villalba_Proyecto_tesis_8.txt
Tamaño del archivo original : 13,99 MB
Número de palabras : 24.289
Número de caracteres : 164824

Depositante : BYRON WLADIMIR OVIEDO BAYAS
Fecha de depósito : 24 de junio de 2026
Tipo de carga : interface
fecha de fin de análisis : 24 de junio de 2026

Santa Elena, 26 de junio de 2026

TUTOR

Validar únicamente en FirmaEC.
Firmado electrónicamente por:
BYRON WLADIMIR
OVIEDO BAYAS

Ing. Byron Wladimir Oviedo Bayas, Ph.D.

UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA
FACULTAD DE SISTEMAS Y TELECOMUNICACIONES
INSTITUTO DE POSTGRADO

AUTORIZACIÓN

Yo, **VILLALBA SOLÍS MÓNICA PAULINA**

Autorizo a la Universidad Estatal Península de Santa Elena, para que haga de este trabajo de titulación o parte de él, un documento disponible para su lectura, consulta y procesos de investigación, según las normas de la Institución.

Cedo los derechos en línea patrimoniales de examen de carácter complexivo con fines de difusión pública, además apruebo la reproducción de este examen de carácter complexivo dentro de las regulaciones de la Universidad, siempre y cuando esta reproducción no suponga una ganancia económica y se realice respetando mis derechos de autor.

Santa Elena, 26 de junio de 2026

EL AUTOR

Validar únicamente en FirmaEC.
Firmado electrónicamente por:
MONICA PAULINA
VILLALBA SOLIS

Villalba Solís Mónica Paulina

AGRADECIMIENTO

A Dios, por brindarme fortaleza, sabiduría y perseverancia para culminar esta etapa académica, a mi esposo, por su apoyo incondicional, comprensión y motivación constante, a mis hijos, quienes son mi mayor inspiración y razón para seguir adelante, a mi madre y a mi familia, por el respaldo y aliento que siempre me brindaron para hacer posible la realización de este trabajo.

De manera especial, agradezco al Gobierno Autónomo Descentralizado Municipal del cantón Salcedo por haberme permitido desarrollar la presente investigación, facilitando el acceso a la información y el contexto institucional necesario para la ejecución de este trabajo académico.

Mónica Paulina, Villalba Solís

DEDICATORIA

Dedico este trabajo a Dios, por ser mi guía, fortaleza y fuente de sabiduría en cada etapa de este camino académico, a mi papá, quién, aunque ya no está físicamente, siempre me orientó para ser la persona que soy, y cuya memoria continúa inspirando cada uno de mis logros, y a mi familia, por su amor, apoyo incondicional y comprensión constante, que fueron fundamentales para superar los retos y culminar con éxito este proceso de formación profesional.

Mónica Paulina, Villalba Solís

ÍNDICE GENERAL

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

RESUMEN

La elevada dependencia de los sistemas de información para gestionar los ingresos públicos en el GAD municipal del cantón Salcedo ha generado vulnerabilidades de ciberseguridad que perjudican la continuidad operativa. El objetivo de este estudio consistió en describir el estado actual de la ciberseguridad en los sistemas de recaudación tributaria, específicamente en aquellos desarrollados internamente, y se excluyó el sistema de AME utilizado para recaudación de impuestos prediales, ya que es una plataforma externa sobre la cual el GAD no posee control directo. Del análisis realizado se encontraron brechas técnicas, organizativas y normativas que sirvieron para la elaboración de un plan de mejora. Para tal efecto, se optó por un alcance Descriptivo–Aplicativo, un diseño no experimental y un enfoque mixto, con un muestreo no probabilístico por conveniencia donde participarán los 7 profesionales del área de TIC. Para la recogida de los datos se recurrió a encuestas, entrevista y análisis normativo. El estudio no evaluó la efectividad real de los controles cumplidos sino la percepción del personal y la evidencia documental existente.

Con base en este diagnóstico, la integración de estándares como ISO/IEC 27001:2022, NIST CSF y la LOPDP favorece el fortalecimiento de los sistemas tributarios. Como resultado, se propone un plan estructurado para mejorar la situación, pero sin que ello suponga una implementación o validación del mismo.

Palabras claves: Ciberseguridad, sistemas tributarios, GAD Municipales.

ABSTRACT

The high dependence on information systems to manage public revenue in the local government of the canton of Salcedo has generated cybersecurity vulnerabilities that harm operational continuity. The objective of this study was to describe the current state of cybersecurity in tax collection systems, specifically those developed internally, the AME system used for property tax collection was excluded from the analysis, as it is an external platform over which the local government has no direct control. From the analysis carried out, technical, organizational, and regulatory gaps were identified as a basis for designing an improvement plan.

For this, a descriptive-applicative scope was chosen, with a non-experimental design and a mixed approach, using non-probabilistic convenience sampling that selected the seven professionals from the IT area. Data collection included surveys, interviews, and regulatory analysis. The study did not evaluate the actual effectiveness of the controls, but rather the staff's perception and the available documentary evidence.

Based on this diagnosis, the integration of standards such as ISO/IEC 27001:2022, NIST CSF, and LOPDP favors the strengthening of tax systems. As a result, a structured plan is proposed to improve the situation, but this does not imply its implementation or validation.

Keywords: Cybersecurity, tax systems, Local Governments.

INTRODUCCIÓN

La creciente dependencia tecnológica de los gobiernos locales para la gestión de los procesos tributarios, ha convertido a la ciberseguridad en un componente esencial para garantizar la continuidad operativa, la protección de los datos y la confianza ciudadana. En ese orden de ideas, los sistemas de recaudación de los impuestos que fueron desarrollados de manera interna por parte del GAD municipal del cantón Salcedo son bienes muy importantes, ya que los mismos son las herramientas que permiten procesar la información financiera y la administrativa de los contribuyentes. Dentro del alcance de este estudio, no se encuentra en el listado de sistemas de recaudación de impuestos urbanos y rurales los que son administrados por la Asociación de Municipalidades Ecuatorianas (AME), ya que pertenece a una plataforma de terceros que no tiene el control directo del GAD.

Con todo, el estado de los sistemas que gestiona los ingresos tributarios muestran debilidades organizativas y técnicas asociadas a la gestión de usuarios, separación de funciones, trazabilidad de las actividades realizadas, seguridad de las bases de datos, la utilización de tecnologías no actualizadas como PHP 5.4.16 (una versión ya no soportada técnicamente) aumenta el riesgo de accesos no autorizados, de pérdida de información, de interrupciones del servicio y de posibles incumplimientos legales, principalmente con la Ley Orgánica de Protección de Datos Personales (LOPDP).

Por ello, la presente investigación tiene como propósito analizar la situación actual de la ciberseguridad en los sistemas de recaudación tributaria desarrollados internamente por el GAD municipal del cantón Salcedo, identificando brechas frente a estándares internacionales para

proponer un plan de fortalecimiento orientado a mitigar vulnerabilidades y proteger los datos institucionales. Para la evaluación se eligió la norma ISO/IEC 27001:2022 y el NIST Cybersecurity Framework, la razón es que estos son los estándares más utilizados en el sector público ecuatoriano, la ISO 27001 aporta un enfoque estructurado de gestión de la seguridad, mientras que el NIST CSF utiliza un lenguaje más sencillo, pensado para que tanto los técnicos como los directivos puedan entenderlo y aplicarlo sin dificultad.

El documento se estructura en varios capítulos. El primero presenta el marco teórico sobre ciberseguridad, estándares internacionales y normativa nacional aplicable. El segundo describe la metodología empleada, para la recolección y análisis de información. El tercero presenta el diagnóstico de la ciberseguridad, el análisis de brechas y finalmente, el plan de fortalecimiento propuesto, seguido de las conclusiones y recomendaciones.

CAPÍTULO I

1. FUNDAMENTACIÓN

1.1 ANTECEDENTES

La gestión tributaria municipal en el Ecuador, ha experimentado un proceso progresivo de digitalización orientado a optimizar la recaudación, mejorar la eficiencia administrativa y facilitar el acceso de los ciudadanos a los servicios públicos. En este contexto, los Gobiernos Autónomos Descentralizados (GAD) han incorporado sistemas informáticos para la administración de catastros, emisión de títulos de crédito y control de obligaciones tributarias. Convirtiendo a la información digital en un activo estratégico para la gestión pública (Andrade, 2022; Calle, 2025).

No obstante, este proceso de transformación digital no siempre ha sido acompañado de una adecuada gestión de la ciberseguridad. Diversos estudios evidencian que la implementación de tecnologías en entidades públicas suele presentar debilidades asociadas a la obsolescencia de la infraestructura, la ausencia de políticas formales de seguridad de la información y la limitada adopción de estándares internacionales, lo que incrementa la exposición a incidentes de seguridad (Boné, 2023; Banco Mundial, 2024).

En el caso concreto del GAD municipal del cantón Salcedo, los mecanismos de recaudación tributaria tienen una arquitectura tecnológica fragmentada; utilizando componentes obsoletos, bases de datos sin configuraciones de seguridad adecuadas y una carencia de controles imprescindibles como la definición de perfiles, la separación de funciones y las audiencias por medio de las pistas de auditoría. Además, se han encontrado versiones obsoletas de PHP 5.4.16 sin soporte desde el año 2015, lo que aumenta la superficie de ataque y expone a los sistemas a vulnerabilidades conocidas, facilitando accesos o ataques por parte de ciberdelincuentes.

Estas condiciones representan riesgos reales de pérdida, alteración o filtración de información tributaria, así como de interrupción de los servicios institucionales, lo que puede afectar la confianza de los contribuyentes y generar implicaciones administrativas y legales para la entidad. Este escenario local se enmarca en una problemática regional más amplia, donde los organismos gubernamentales de América Latina se han convertido en uno de los principales objetivos de ciberataques, debido a su baja madurez en seguridad, limitaciones presupuestarias y escasez de personal especializado (Check Point Research, 2025; PT Cyber Analytics, 2025).

En el medio ecuatoriano, tal situación se ve multiplicada por las exigencias que la Ley Orgánica de Protección de Datos Personales (LOPDP) pone a las instituciones del sector público, las cuales están obligadas a adoptar medidas técnicas y organizacionales adecuadas para garantizar que los datos personales estén protegidos, no sean alterados y estén disponibles cuando se necesiten. Sin embargo, las investigaciones orientadas a la gestión tributaria y a la transformación digital de los gobiernos locales dejan en claro la existencia de importantes brechas que separan los requerimientos normativos de las prácticas reales implementadas, sobre todo en lo relacionado con la gestión de riesgos y controles de seguridad de la información. (Cabezas, 2025; Morán Chilán & Pangay Sánchez, 2025).

Desde el punto de vista académico, la repercusión de la digitalización en la recaudación tributaria, en todo caso, ha sido analizada por diferentes estudios que concluyeron que por un lado se logró un avance en cuanto a las mejoras operativas y financieras y, por otro lado, se han evidenciado dificultades en la protección de la información y la seguridad de los sistemas tributarios (Elizalde Salazar, 2025; Pico González et al., 2024) y por investigaciones sobre ciberseguridad en sistemas empresariales y financieros, para las cuales la falta de alineación con

los estándares internacionales como la ISO/IEC 27001 y ante los marcos de referencia como el NIST Cybersecurity Framework harán que la capacidad de las organizaciones para prevenir, detectar y responder frente a los incidentes de seguridad se vea limitada (Murillo, 2022; Boné, 2023).

A pesar de la existencia de tales antecedentes, se observa escasa producción científica académica donde se analice la ciberseguridad de los sistemas tributarios de los gobiernos municipales ecuatorianos. Este sería el diagnóstico de la situación respecto a un diagnóstico fundamentado en estándares internacionales y normativa nacional, lo que da razón de ser, el llevar a cabo investigaciones que estén contextualizadas adecuadamente, que comprendan la realidad institucional de los GADs y que contemplen propuestas de solución prácticas e instrumentales que lleven consigo el fortalecimiento de la seguridad de la información.

De este modo, la investigación realizada se justifica en la necesidad de analizar de forma exhaustiva la ciberseguridad en los sistemas tributarios del GAD municipal del cantón Salcedo, tomando como referencia estándares internacionales y buenas prácticas reconocidas con la intención de poder detectar las brechas, evaluar el impacto y diseñar un plan de fortalecimiento que contribuya a la resiliencia digital y el cumplimiento normativo de la institución.

1.2 DESCRIPCIÓN DEL PROYECTO

El presente proyecto se orienta al análisis y fortalecimiento de la ciberseguridad en los sistemas de recaudación tributaria del Gobierno Autónomo Descentralizado Municipal del cantón Salcedo, considerando la creciente dependencia institucional de las tecnologías de la información para la gestión de los ingresos públicos y la protección de datos sensibles. La investigación parte de un diagnóstico del estado actual de la seguridad de la información, con el propósito de

identificar brechas técnicas, organizativas y normativas que afectan la confidencialidad, integridad y disponibilidad de los datos tributarios administrados por la institución.

El trabajo se desarrolla según la investigación correspondiente a la línea de investigación Tecnología y Sistemas de la Información (TSI), en concreto, con las sublíneas de TSI en las organizaciones y la sociedad y Redes y Seguridad de la Información, como eje referencial desde donde se identifica el problema, la formulación de la pregunta de investigación y la definición del objeto de estudio presente en este texto; desde esta perspectiva, se examina la forma de relación que existe entre el grado de cumplimiento de los estándares de seguridad de la información y la forma de protección de los sistemas tributarios municipales, así como la gestión de los riesgos digítales en el GAD municipal del cantón de Salcedo.

Para poder llevar a cabo el proyecto, se utilizó un diseño metodológico adecuado no experimental, con un alcance descriptivo - aplicativo y un enfoque mixto, ya que permite observar la realidad institucional sin alterar los procesos de operación. La información se recolectó siguiendo encuestas estructuradas dirigidas al personal de la Jefatura de Tecnologías de la Información y Comunicación (TIC), de un test tipo Likert, utilizando estándares internacionales como ISO/IEC 27001:2022, el NIST Cybersecurity Framework y la normativa nacional en vigor, según la Ley Orgánica de Protección de Datos Personales (LOPDP); así como por una entrevista estructurada a un experto en ciberseguridad que ayuda a complementar el diagnóstico, cuya mirada es especial desde la técnica.

Con los resultados obtenidos del diagnóstico se propone el diseño de un plan de fortalecimiento de la ciberseguridad orientado a mitigar las vulnerabilidades, a mejorar los controles de seguridad y a garantizar que la información tributaria sea confidencial, integra y esté

disponible, tal como se apoyan las buenas prácticas internacionales y los requerimientos normativos del sector público, siempre con un enfoque práctico y sobre la realidad operativa del GAD municipal del cantón Salcedo.

Con relación a esta consideración, el proyecto no se detiene aquí, ya que no se propone simplemente describir el estado de situación en la ciberseguridad institucional, sino que también prevé la aportación de una propuesta técnica y organizativa, la cual tendrá la consideración de una herramienta de apoyo a la toma de decisiones y contribuirá al fortalecimiento de la resiliencia digital del gobierno local, al tiempo que ayuda a la satisfacción de las obligaciones legales y administrativas en materia de protección de la información.

1.3 OBJETIVOS DEL PROYECTO

1.3.1 OBJETIVO GENERAL

Analizar el estado actual de la ciberseguridad en los sistemas tributarios del GAD municipal del cantón Salcedo, considerando el nivel de cumplimiento de los estándares de seguridad y las brechas existentes, como base para el diseño de un plan de fortalecimiento orientado a la mitigación de vulnerabilidades y a la protección de la confidencialidad, integridad y disponibilidad de la información.

1.3.2 OBJETIVOS ESPECÍFICOS

- Diagnosticar el estado actual de la ciberseguridad en los sistemas tributarios, identificando el nivel de cumplimiento respecto a los estándares de seguridad de la información y las brechas existentes que afectan la protección de los datos institucionales.

- Definir los lineamientos técnicos y normativos que orienten el fortalecimiento de la seguridad de la información, fundamentados en los resultados del diagnóstico y en las buenas prácticas establecidas por los marcos internacionales y la normativa aplicable.
- Diseñar un plan de fortalecimiento de la ciberseguridad para los sistemas tributarios del GAD municipal del cantón Salcedo, incorporando controles, acciones y criterios orientados a la mitigación de vulnerabilidades y al aseguramiento de la confidencialidad, integridad y disponibilidad de la información

1.4 JUSTIFICACIÓN DEL PROYECTO

La presente investigación se justifica por la necesidad de fortalecer la ciberseguridad en los sistemas de recaudación tributaria del Gobierno Autónomo Descentralizado Municipal del cantón Salcedo, debido a la criticidad de la información que estos gestionan y a las debilidades identificadas en su infraestructura tecnológica y controles de seguridad. La presencia de partes desactualizadas, de configuraciones insuficientes y de la falta de mecanismos formales de control incrementa el riesgo de incidentes que pueden afectar la confidencialidad, integridad y disponibilidad de la información de la institución.

Al mismo tiempo, el proyecto se considera adecuado en relación a lo que establece la Ley Orgánica de Protección de Datos Personales, que obliga a las administraciones públicas a llevar a cabo una serie de medidas técnicas y organizativas para proteger la información. Y en este sentido, la investigación permite evaluar el nivel de cumplimiento normativo y establecer acciones de mejora con carácter volitivo, de acuerdo con estándares de internacionalización con metas en seguridad de la información como la ISO/IEC 27001:2022 y el NIST Cybersecurity Framework. Desde la opción legal, es relevante mencionar que la investigación aquí presentada tiene un ámbito

académico, no jurídico, como sugiere el carácter preliminar, así como, no establece responsabilidades concretas a la institución o a sus funcionarios, sin embargo, colindante a los resultados ya presentados se puede aseverar la existencia de riesgos potenciales que, de no ser atendidos, podrían dar lugar a situaciones administrativas o jurídicas. Como ejemplo, la falta de controles de seguridad, la falta de mecanismos de trazabilidad, dificultaría, en un contexto real, la determinación de responsabilidades ante un incidente, dificultando a la vez la transparencia institucional y generando reclamaciones por parte de los ciudadanos. Por tanto, el valor del trabajo no está en emitir o realizar un juicio justo sino en alertar acerca de escenarios que la institución debería considerar para hacer ciberseguridad y para conformar el riesgo de sanciones o conflictos.

Desde el ámbito profesional y social, el desarrollo del proyecto contribuye a mejorar la gestión de riesgos digitales, fortalecer la confianza ciudadana y apoyar la toma de decisiones institucionales mediante el diseño de un plan de fortalecimiento de la ciberseguridad, aplicable a los sistemas tributarios municipales y replicable en otros gobiernos locales.

1.5 ALCANCE DEL PROYECTO

El presente proyecto analiza el estado actual de la ciberseguridad en los sistemas de recaudación tributaria desarrollados internamente para la gestión de ingresos municipales, tales como agua potable, alcantarillado, comerciantes de plazas, arrendamientos, contribución especial de mejoras, regalías mineras, recolección de desechos sólidos, cementerio, impuesto al juego, activos y patentes. Estos sistemas funcionan de manera separada, cada tributo cuenta con su propio sistema independiente y una base de datos propia, sin una plataforma unificada, lo que fragmenta la gestión y dificulta la aplicación homogénea de controles de seguridad.

Se deja fuera del análisis el sistema de recaudación de impuestos urbanos y rurales, ya que se trata de una plataforma de terceros creada por la Asociación de Municipalidades Ecuatorianas (AME), sobre la cual el GAD no tiene control directo en su desarrollo ni en su arquitectura tecnológica. Esta exclusión no afecta el análisis de brechas, puesto que la investigación se centra únicamente en los sistemas que han sido desarrollados y gestionados internamente por la institución, es decir, aquellos que el GAD puede evaluar, administrar y proponer mejoras. De este modo, los resultados obtenidos evidencian las debilidades y necesidades de fortalecimiento del entorno tecnológico que es de la responsabilidad directa del GAD.

La investigación se restringe funcionalmente a la Jefatura de Tecnologías de la Información y Comunicación (TIC) del GAD municipal del cantón Salcedo y considerando para ello al personal que lleva a cabo de forma directa la operación, gestión y seguridad de los sistemas tributarios. Por lo que también incluye aspectos técnicos y organizativos, y la gestión de los accesos, roles de usuario, validaciones de seguridad, controles de auditoría y cumplimiento de políticas organizativas internas.

En lo que respecta a la normativa y la referencia, el proyecto solo se ocupa de verificar el cumplimiento de los estándares internacionales ISO/IEC 27001:2022 e ISO/IEC 27002:2022, y el NIST Cybersecurity Framework y también de la Ley Orgánica de Protección de Datos Personales, como normativa nacional, sino que también incluye el diagnóstico del proyecto de los resultados, diseñado para fortalecer la ciberseguridad, pero no la implementación, pruebas técnicas ni el funcionamiento del mismo.

CAPÍTULO II

2. MARCO TEORÍCO Y METODOLOGÍA DEL PROYECTO

2.1 MARCO TEÓRICO

El marco teórico contempla el fundamento conceptual, las teorías y antecedentes que permiten entender la problemática de la ciberseguridad en los sistemas tributarios municipales, y sirve de base para el desarrollo de la propuesta y el análisis desarrollado. En este apartado se desarrollan temas como, la ciberseguridad, la seguridad de la información, la transformación digital, la gestión de riesgos, la aplicación de estándares internacionales (Andrade, 2022; Calle, 2025).

La ciberseguridad se entiende como el conjunto de políticas, procesos, prácticas y tecnologías diseñadas a proteger los sistemas de información, redes, aplicaciones y datos frente a amenazas internas o externas, que puedan comprometer el funcionamiento y la seguridad de estos sistemas. Con el aumento de la digitalización, las organizaciones dependen cada vez más de los entornos tecnológicos para sus procesos más críticos, lo que hace indispensable a la ciberseguridad (Boné, 2023). En el plano institucional, no sólo estamos hablando de soluciones tecnológicas, sino de dimensiones organizativas, humanas y normativas que permiten gestionar los riesgos de forma integral (Banco Mundial, 2024).

La seguridad de la información, por su parte, persigue la protección de la información, independientemente del soporte o su forma, sea esta digital, física o verbal, asegurando la confidencialidad, la integridad y la disponibilidad de la misma, principios que constituyen el sustento de los sistemas de gestión de seguridad de la información, y de los estándares de los

marcos de referencia internacionales, aplicados tanto al sector público como al privado (Murillo, 2022).

En las organizaciones públicas, la seguridad de la información y la ciberseguridad adquieren un valor estratégico, debido a la gran cantidad y sensibilidad de los datos que manejan, sean estos: personales, financieros, tributarios, administrativos. La exposición, alteración o pérdida de esta información puede generar graves impactos técnicos, legales, económicos y sociales, e incluso afectar la confianza ciudadana y la credibilidad institucional (Morán y Pangay, 2025).

De modo que, de acuerdo con este planteamiento, la ciberseguridad no es más que una parte específica de la seguridad de la información. La seguridad de la información protege la información independientemente de su formato, sea digital o físico o mediante documentos; la ciberseguridad protege la información conforme a los riesgos que tiene asociados el entorno digital que está conectado a redes (Murillo, 2022); Tal separación es fundamental para separar las debilidades comunes de la información y el tipo de vulnerabilidad técnica de la infraestructura.

La transformación digital en el sector público ha promovido el uso de sistemas informáticos para optimizar la gestión administrativa, mejorar la recaudación tributaria y facilitar el acceso de los ciudadanos a los servicios públicos. A nivel municipal, los sistemas tributarios permiten gestionar catastros, emitir títulos de crédito, controlar pagos, y generar informes financieros. Diversas investigaciones coinciden en que, la digitalización tributaria es la responsable de mejorar los procesos, aunque también incrementan los riesgos de seguridad cuando no se aplican controles adecuados (Pico et al., 2024; Elizalde, 2025).

Los sistemas tributarios municipales almacenan información crítica para la sostenibilidad financiera y operativa de los gobiernos municipales. Entre los principales riesgos asociados a la seguridad se encuentra el acceso no autorizado a bases de datos, la manipulación de la información financiera, la indisponibilidad de servicios por ataques cibernéticos y la explotación de vulnerabilidades en software desactualizado (Check Point Research, 2025; PT Cyber Analytics, 2025).

La gestión de riesgos en ciberseguridad se postula como una herramienta clave para proteger los sistemas de información en el sector público. Esto es identificar, analizar y evaluar el riesgo de los activos de información, así como establecer y ejecutar controles para su mitigación. Esto permite priorizar las acciones de seguridad, de acuerdo con el impacto y la probabilidad de los incidentes, optimizando los recursos existentes y aumentando la resiliencia organizativa ante eventos adversos (ISO/CEI, 2022). Los estándares internacionales en materia de seguridad de la información, tal y como es la norma ISO/IEC 27001:2022 y el marco referencia NIST Cybersecurity Framework, establecen recomendaciones para pautar la implementación de políticas, procedimientos y controles dirigidos a proteger la información y la mejora continua de la seguridad informática, en especial la ciberseguridad. Cuando las instituciones públicas adoptan estándares de información, no sólo alinean su organización con las prácticas nacionales de seguridad, sino que también acompañan el cumplimiento de los requisitos normativos nacionales (Banco Mundial, 2024).

El marco teórico también incorpora el enfoque legal vigente en Ecuador, en particular la Ley Orgánica de Protección de Datos Personales, que establece obligaciones específicas para las instituciones públicas en materia de seguridad de la información, gestión de riesgos y protección

de los derechos de los titulares de datos. La articulación entre los estándares internacionales y la normativa nacional es muy importante para una gestión integral de la ciberseguridad en los sistemas tributarios municipales (Asamblea Nacional del Ecuador, 2021).

En el contexto de los sistemas tributarios municipales, la seguridad de la información garantiza que los datos financieros y personales de los contribuyentes se mantengan confidenciales, íntegros y disponibles. La ciberseguridad, en cambio, protege estos sistemas de ataques activos que podrían interrumpir el servicio, robar información o comprometer la infraestructura tecnológica.

En definitiva, el marco teórico permite comprender la importancia de la ciberseguridad y la seguridad de la información en los sistemas tributarios del sector público, identificar los principales riesgos derivados de la digitalización y justificar el uso de los estándares internacionales como base para el diseño del plan de fortalecimiento de la ciberseguridad en el GAD municipal del cantón Salcedo.

2.1.1 MARCO CONCEPTUAL

La ciberseguridad se define como un conjunto de políticas, procesos, prácticas y tecnologías enfocadas en salvaguardar los sistemas de información, las redes y los datos contra amenazas tanto internas como externas que podrían comprometer su seguridad y operatividad (Boné, 2023; Banco Mundial, 2024).

La seguridad de la información se ocupa de proteger la información sin importar su formato, asegurando el cumplimiento de los principios de confidencialidad, integridad y disponibilidad (Murillo, 2022). Desde esta perspectiva, si bien estos conceptos suelen recurrirse

de forma indistinta, la ciberseguridad puede observarse, en un sentido delimitado, como un subgrupo especializado en el marco de la seguridad de la información.

La madurez de la ciberseguridad es la habilidad o grado de preparación que tiene cada institución para defender sus activos y su información de ciberataques. Cuando la madurez sea madura, robusta, podrá mitigar mejor los ciberataques o amenazas digitales.

Este enfoque se conoce como el modelo CIA (por sus siglas en inglés: Confidentiality, Integrity and Availability), que aborda dichos principios, y son la base conceptual para la seguridad de la información. La confidencialidad busca que la información solo sea accesible por la persona o personas, los sistemas o procesos debidamente autorizados. La integridad tiene como objetivo garantizar que los datos sean completos y exactos, con la dificultad de las modificaciones no autorizadas. La disponibilidad implica que la información y los sistemas deben estar accesibles para cumplir con los objetivos institucionales cuando sea necesario (ISO, 2022; National Institute of Standards and Technology [NIST], 2024). Estos principios son los que guían el diseño e implementación de controles en seguridad de la información.

La Organización Internacional de Normalización (ISO, 2022) define un activo de información como cualquier componente que tenga valor para la entidad y que necesite una protección apropiada ante peligros internos o externos. Estos activos pueden abarcar aplicaciones informáticas, datos digitales, infraestructura tecnológica, procesos institucionales, bases de datos, documentación física y recursos humanos que están relacionados con la gestión de la información. Se hace imprescindible que un Sistema de Gestión de Seguridad de la Información (SGSI) pueda identificar y clasificar los activos, ya que esto ayuda a determinar la importancia de los activos y, en consecuencia, añade los controles oportunos en función del nivel de riesgo.

El concepto de "sistemas municipales" también es un concepto fundamental, y hace referencia a la suma total de aplicaciones informáticas, bases de datos y métodos tecnológicos que utilizan los gobiernos locales con la finalidad de gestionar la recaudación de impuestos, administrar los catastros y producir la información financiera. Como estos sistemas actúan como almacenamiento de información sensible de tipo económico y personal, resulta importante y necesario protegerlos para lograr la confianza del ciudadano y garantizar una continuidad de las instituciones (Andrade, 2022).

Así, el proceso sistemático para detectar, identificar y valorar los riesgos que tienen influencia en los recursos informáticos se denomina gestión de riesgos de ciberseguridad, siendo su finalidad establecer controles que permitan reducir la probabilidad de que los mismos se concretan en la práctica y de su severidad. Este modelo es de vital importancia en los organismos públicos, donde los límites de recursos se ven obligados a determinar qué acciones de seguridad se van a priorizar en función de la magnitud del riesgo. (ISO/IEC, 2022).

Por último, los estándares internacionales de seguridad de la información son marcos de referencia que guían a las organizaciones en la adopción de prácticas seguras adecuadas. La norma ISO/IEC 27001:2022 y el NIST Cybersecurity Framework son los más destacados para este estudio, ya que ofrecen directrices para la mejora constante de la ciberseguridad y la protección de la información.

2.1.2 MARCO REFERENCIAL

El marco referencial, también denominado estado del arte, recoge los principales estudios y antecedentes relacionados con la ciberseguridad, la transformación digital y la gestión tributaria en el ámbito de los gobiernos locales. Diversas investigaciones evidencian que la digitalización de

los procesos tributarios ha permitido mejorar la eficiencia administrativa y la recaudación de ingresos municipales; pero también, ha incrementado los riesgos asociados a la seguridad de la información cuando no se adoptan controles adecuados. (Calle, 2025; Pico et al., 2024).

La falta de políticas oficiales de seguridad, la escasa formación del personal y las infraestructuras tecnológicas desactualizadas son debilidades en ciberseguridad que presentan los gobiernos locales, según investigaciones efectuadas en Ecuador y Latinoamérica (Morán y Pangay, 2025). Por otra parte, los estudios sobre la ciberseguridad institucional subrayan que la incapacidad de las organizaciones para prevenir, detectar y responder a incidentes de seguridad se reduce cuando no se alinean con normas internacionales como el marco NIST de Ciberseguridad y la ISO/IEC 27001. (Murillo, 2022; Boné, 2023).

De acuerdo con la documentación de varias entidades internacionales, estas se han convertido, en las últimas fechas, en uno de los blancos más relevantes de ataques informados, debido a su bajo nivel de madurez en términos de ciberseguridad y al descenso progresivo que ha habido en los últimos años en la digitalización de sus servicios (Banco Mundial, 2024; Check Point Research, 2025). Pese a lo anterior, existe escasa producción académica que tenga por objeto el estudio de la ciberseguridad de los sistemas tributarios de los municipios de Ecuador. Esto se traduce en una debilidad en este eje temático, el cual es el eje central del presente desarrollo.

La revisión sistemática se llevó a cabo conforme a las directrices PRISMA (Preferred Reporting Items for Systematic Reviews and Meta-Analyses) 2020, que es un estándar global para la elaboración y presentación de revisiones sistemáticas de literatura. Esta forma de proceder permite asegurar la transparencia, la reproducibilidad y el rigor científico del proceso de búsqueda,

selección y análisis de la evidencia asociada a la ciberseguridad en los sistemas tributarios municipales.

La búsqueda bibliográfica se realizó en bases de datos académicas y repositorios científicos, entre ellos se incluyeron Scopus y Web of Science, por su cobertura de literatura científica, IEEE Xplore, especializada en ingeniería, ciencias de la computación y tecnología, ScienceDirect, que proporciona acceso a revistas científicas y libros académicos, Google Scholar como motor de búsqueda multidisciplinario, y repositorios universitarios de instituciones ecuatorianas y latinoamericanas, con el fin de incorporar investigaciones contextualizadas y antecedentes académicos relacionados con la temática del estudio.

Los criterios de elegibilidad se determinan en la siguiente tabla:

Tabla 1. Criterio de elegibilidad para matriz prisma

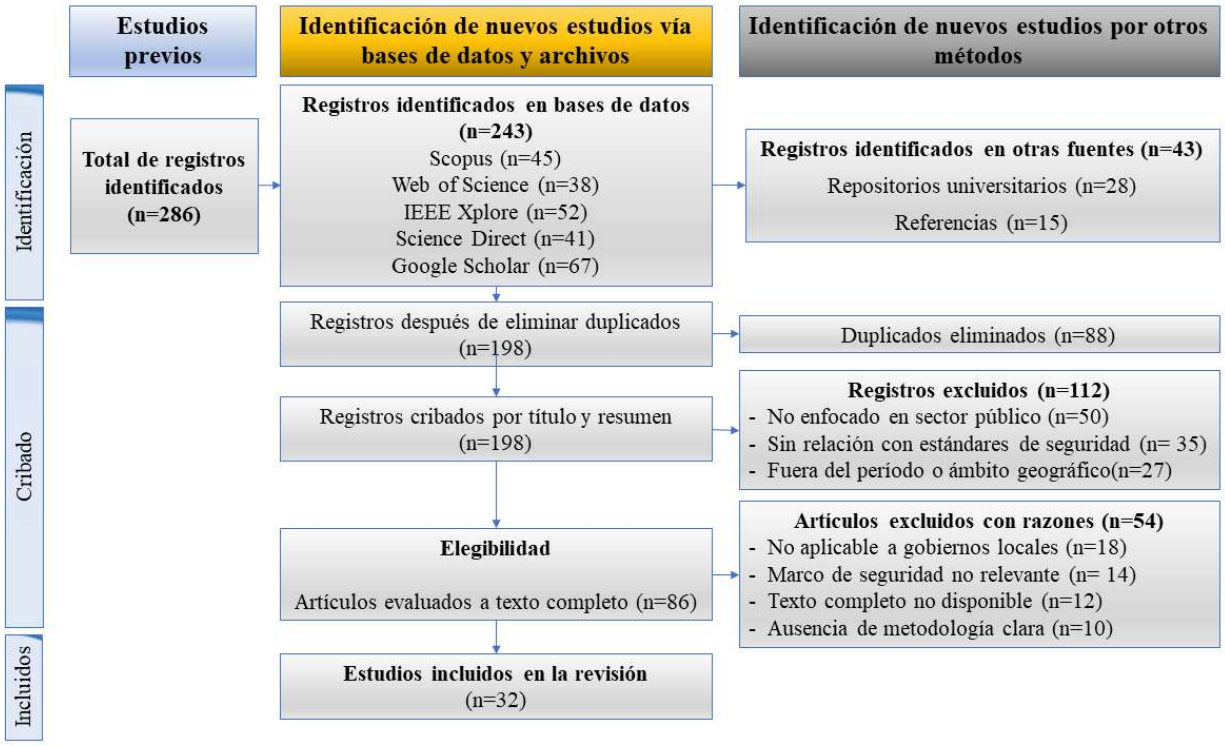
Criterios de Inclusión	Criterios de Exclusión
Publicación: Artículos, actas de congresos o tesis de posgrado publicados entre 2019 y 2025.	Publicaciones anteriores a 2019.
Idioma: Textos completos disponibles en español o inglés.	Textos en otros idiomas o cuyo texto completo no esté accesible.
Criterios de calidad: Literatura que ha sido sometida a revisión por pares, ya sea en revistas o conferencias, así como trabajos de fin de máster o doctorado provenientes de universidades acreditadas.	Fuentes no verificadas, publicaciones en blogs y reportes informales carentes de un enfoque metodológico estructurado.

Tema principal: Investigación sobre ciberseguridad y protección de la información en el ámbito del sector público o en los gobiernos locales.	Estudios vinculados a la digitalización fiscal y la eficacia administrativa, aunque sin un enfoque específico en la seguridad y los riesgos.
Marco de referencia: Estudios que se fundamentan en la utilización, evaluación y sugerencias de marcos, normativas o mecanismos de seguridad, tales como: ISO/IEC 27001, NIST CSF, CIS y regulaciones locales.	Estudios que no se relacionen, no mencionen, no utilicen o no evalúen estándares, marcos o controles de seguridad de la información.
Alcance geográfico e institucional: Estudios que sean aplicados a gobiernos locales o municipales, entidades públicas en países en desarrollo, o contextos que sean similares o análogos al ecuatoriano.	Estudios realizados en ámbitos privados, como banca y comercios al por menor; o de gobierno nacional o central, sin que se relacionen con el nivel local.
Tipo de estudios: Investigaciones experimentales, diagnósticos, estudios de caso, revisiones sistemáticas o propuestas de modelos y planes.	Editoriales, opiniones, predicciones futurológicas o estudios puramente teóricos sin aplicación o validación contextual.

Nota*:* Datos obtenidos para desarrollo de diagrama prisma

El siguiente diagrama presenta el flujo de selección de estudios siguiendo las directrices PRISMA 2020:

Figura 1 . Diagrama de flujo PRISMA de la revisión bibliográfica



Nota. La búsqueda se realizó considerando publicaciones de los últimos 6 años (2019-2025)

En la siguiente tabla se presenta el resumen cuantitativo del proceso de selección de estudios. Los porcentajes fueron calculados considerando como base el total de registros correspondientes a cada fase del proceso: identificación, cribado y elegibilidad, con el fin de mantener coherencia metodológica en la interpretación de los registros analizados.

Tabla 2. Resumen del proceso de selección

Fases del proceso	Cantidad de registros	Distribución Porcentual	Porcentaje
IDENTIFICACIÓN			
Registros identificados en bases de datos	243	85%	
Registros identificados en otras fuentes	43	15%	

Total de registros identificados	**286**		**100%**
Cribado			
Duplicados eliminados	88	30.77%	
Registros para cribado (título/resumen)	198	69.23%	
(registros: 198=100%)			
Registros excluidos en cribado	**112**		**56.57%**
• No enfocado en sector público	50	25.25%	
• Sin relación con estándares de seguridad	35	17.68%	
• Fuera del período o ámbito geográfico	27	13.64%	
Registros que pasan a elegibilidad	**86**		**43.43%**
ELEGIBILIDAD			
Artículos evaluados a texto completo	86		**100%**
Artículos excluidos con razones	**54**		**62.79%**
• No aplicable a gobiernos locales	18	20.93%	
• Marco de seguridad no relevante	14	16.28%	
• Texto completo no disponible	12	13.95%	
• Ausencia de metodología clara	10	11.63%	
Inclusión			
Estudios incluidos en la revisión	32		**37.21%**

Nota: Se muestra la cantidad de registros determinados en la revisión bibliografía. Los porcentajes de cribado y elegibilidad corresponden al total de registros de la fase anterior

2.1.3 MARCO LEGAL

El marco legal de la investigación se fundamenta en la normativa ecuatoriana vigente relacionada con la protección de la información y los datos personales. En este sentido, la LOPDP

establece las disposiciones que regulan el tratamiento de datos personales en el sector público y privado, imponiendo a las instituciones públicas la obligación de implementar medidas técnicas y organizativas que garanticen la confidencialidad, integridad y disponibilidad de la información (Asamblea Nacional del Ecuador, 2021).

La LOPDP tiene varios principios, entre ellos, la licitud, la lealtad, la transparencia, el principio de la minimización de datos, la seguridad, que se deben observar por parte de las entidades públicas en el tratamiento de la información de carácter personal. El Reglamento General de la LOPDP, contiene disposiciones específicas sobre las medidas de seguridad técnicas y organizativas que deben implementar las instituciones públicas, así como la gestión de riesgos, la notificación de incidentes de seguridad, los controles de acceso y la trazabilidad de las operaciones con datos personales. Aspectos que van directamente relacionados con la ciberseguridad de los sistemas tributarios municipales.

Además de la LOPDP y su reglamento, el marco jurídico de los sistemas tributarios municipales se encuentra en el Código Orgánico de Organización Territorial, Autonomía y Descentralización (COOTAD), que establece la autonomía política, administrativa y financiera de los GAD y se adecue la misma directamente a sus competencias legislativas de poder crear y gestionar tributos en sus respectivas circunscripciones territoriales. En dicho sentido, también se reconocen las competencias tributarias de los GAD municipales al igual que la gestión de los impuestos, tasas y contribuciones especiales de mejoras. Tal asunción de competencias tributarias está en conexión directa con los sistemas de recaudación tributaria que son objeto de análisis de la presente investigación, hoy que son los sistemas de información mediante los cuales el GAD ejerce el control de la gestión de los ingresos públicos.

La relación que existe entre la normativa nacional y con el marco validante internacional, permite la potenciación de las capacidades de las instituciones públicas para la protección de la información y el cumplimiento de las responsabilidades que plantean.

Razón por la que la presente investigación considera la LOPDP y su reglamento como un eje fundamental para el análisis del estado actual de la ciberseguridad y para el diseño del plan de fortalecimiento propuesto para el GAD municipal del cantón Salcedo.

2.2 METODOLOGÍA DEL PROYECTO

La metodología del proyecto define de manera sistemática el conjunto de procedimientos, técnicas e instrumentos empleados para el desarrollo de la investigación, con el propósito de analizar el estado actual de la ciberseguridad en los sistemas tributarios del Gobierno Autónomo Descentralizado municipal del cantón Salcedo y establecer los requerimientos que viabilicen el diseño de un plan de fortalecimiento, alineado con estándares internacionales de seguridad de la información.

Por lo que respecta a la metodología que se aplica al caso presente, esta contiene un proceso estructurado centrado de la siguiente manera: por un lado, con la identificación de los sistemas tributarios institucionales que consideran activos críticos, entre los activos críticos de la gestión pública, y, por otro, el análisis de la situación del entorno relativo a la tecnología y de la situación organizativa, con la finalidad de tomar conciencia de la arquitectura de los sistemas, de los flujos de información, de los mecanismos de control existentes.

La propuesta finalmente terminó de definir los criterios de evaluación, desde la siguiente perspectiva: la elaboración de un conjunto de criterios para la evaluación, en torno a estándares de

evaluación, que serán, por ejemplo, ISO/IEC 27001:2022 [48], el NIST Cybersecurity Framework [21] o la normativa nacional aplicable. La validación práctica de los criterios definidos, por medio de técnicas de recogida de información, permitió determinar el grado de adecuación de los controles de seguridad, manifestándose en consecuencia las brechas respecto de la gestión de la ciberseguridad institucional.

En este mismo sentido, la evaluación realizada a cabo sobre los controles y prácticas de seguridad existentes, fue una buena forma de conocer la situación general de los mismos, pero también fue el punto de partida para poder realizar el plan de trabajo en el que se incluyen las medidas de fortalecimiento ante la reducción de los riesgos para la mejora de la protección de la información institucional. Esta sección describe además el tipo de investigación y el diseño de ella, las técnicas de recolección de la información y los grupos poblacionales en los que se realizó la intervención, pero al mismo tiempo garantizando la rigurosidad científica y la coherencia con los objetivos planteados.

2.2.1 METODOLOGÍA DE INVESTIGACIÓN

La investigación se sitúa en el ámbito de un alcance aplicado y descriptivo. Se trata de un alcance descriptivo porque pretende identificar y caracterizar la realidad de la ciberseguridad en los sistemas tributarios municipales, para ello se analiza los controles que se han aplicado y su nivel de cumplimiento asociado a estándares internacionales, mientras que se presenta como un alcance aplicado porque los resultados del análisis no sólo lo permiten describir la problemática, sino que además permiten identificar fallas en la gobernanza, gestión de los incidentes y control de accesos, lo cual constituye insumos de gran valor para poder elaborar una propuesta de mejora.

La metodología adoptada, permite la comparación entre la situación de partida de los sistemas y los criterios definidos en los estándares, permitiendo la detección de brechas de seguridad y priorizando la intervención. En esta línea, los resultados que se obtienen son canalizados hacia propuestas de solución, estructuradas en un plan de refuerzo que integra medidas técnicas, organizativas y normativas acordes con las buenas prácticas internacionales de ciberseguridad.

2.2.2 TÉCNICAS DE RECOLECCIÓN DE INFORMACIÓN

Para la recolección de información se emplearon técnicas de carácter cuantitativo y cualitativo, con el fin de obtener una visión integral de la situación de la ciberseguridad en la institución. Como técnica cuantitativa se utilizó la encuesta aplicada mediante un cuestionario estructurado con escala tipo Likert, el detalle de la encuesta se presenta en el Anexo A. Este instrumento se encuentra basado en los controles y dominios establecidos por la norma ISO/IEC 27001:2022 y en las funciones del NIST Cybersecurity Framework, permitiendo medir el nivel de cumplimiento de las prácticas de seguridad de la información en los sistemas tributarios municipales (ISO/IEC, 2022; NIST, 2024).

La información que se obtiene de las respuestas a la encuesta se tradujo en una escala de 1 a 5, de modo que cada número representa un nivel de percepción. Esto permite transformar las respuestas de cada una de las personas que completaron la encuesta en datos numéricos, lo que facilita su análisis. Aunque son datos que ya tienen un orden, de menor a mayor nivel de percepción, no se trata de datos exactos como puedan ser el tiempo, la cantidad, y se consideran datos cuantitativos ordinales. Dicha codificación numérica permite hacer un uso de las técnicas

estadísticas descriptivas mediante el cálculo de medios para obtener así tendencias generalizadas y establecer comparativas del nivel de percepción de las dimensiones evaluadas.

Pensando un poco en la forma de poder dar sentido a los resultados obtenidos, se construye un baremo con los rangos de medios que permitirán clasificar los valores obtenidos de manera cualitativa en niveles como muy bajo, bajo, medio, alto y muy alto. Este procedimiento que se adopta nos permitió comprender de forma más clara cuál es el grado de implementación de los controles de seguridad en el momento en que se tradujeron los resultados numéricos en categorías interpretativas.

El análisis de confiabilidad del instrumento se realizó mediante el coeficiente Alfa de Cronbach, obteniéndose un valor de 0.715 para las preguntas del cuestionario, lo cual indica una consistencia interna aceptable, lo cual es suficiente para un estudio de tipo diagnóstico y aplicado como el presente caso. Este valor no alcanzó umbrales superiores, no porque el instrumento tenga problemas, sino por características propias del diseño de la investigación que son normales en estudios de caso con poblaciones pequeñas y especializadas.

El coeficiente Alfa de Cronbach es sensible a la longitud de la escala, con solo tres ítems por cada dimensión evaluada (Gobernanza, Control de Acceso, Gestión de Incidentes y Capacitación), es estadísticamente más difícil alcanzar valores muy altos, incluso cuando los ítems están bien diseñados y correlacionados entre sí. Un mayor número de preguntas por dimensión podría haber elevado el coeficiente, pero ello habría alargado innecesariamente el cuestionario sin agregar valor sustancial al diagnóstico.

Luego, el reducido tamaño de la muestra fue la decisión correcta para este estudio, ya que se buscaba incluir a la totalidad del personal TIC. Sin embargo, las pruebas de confiabilidad como el Alfa de Cronbach se comportan de manera más estable con muestras más grandes. Con una muestra pequeña, la estimación estadística es más exigente y tiende a producir valores más modestos, aunque el instrumento sea conceptualmente sólido.

Por lo tanto, el valor de 0.715 es coherente con las características del estudio y, al superar el umbral mínimo de 0.7, respalda plenamente la consistencia interna del instrumento para los fines de esta investigación, esta evidencia se visualiza en el Anexo D. De manera complementaria, como técnica cualitativa se emplea la entrevista estructurada dirigida a un experto en ciberseguridad, con el propósito de obtener criterios técnicos especializados que permitan validar los resultados del diagnóstico y enriquecer el análisis desde una perspectiva profesional, el detalle de la entrevista se presenta en el Anexo B.

Conjuntamente, se incluyen variables sociodemográficas en forma de carga, tiempo de servicio y formación, las cuales se corresponden a datos cualitativos, ya que describen características del personal; algunos no siguen un orden específico como el cargo o la formación (datos nominales), pero otras como el tiempo de servicio sí presentan un orden específico (datos ordinales). Estas variables tienen la utilidad de contextualizar los resultados, pero no se utilizan para calcular medios.

2.2.3 GRUPOS POBLACIONALES INVOLUCRADOS

La población objeto de estudio está conformada por el personal de la Jefatura de Tecnologías de la Información y Comunicación (TIC) del GAD municipal del cantón Salcedo, por su participación directa en la administración, operación y seguridad de los sistemas tributarios

institucionales. Esta población está compuesta por un total de siete funcionarios, que son los encargados de estos procesos.

Se optó por un muestreo censal, es decir, se incluyó a todos los integrantes de la población, por varias razones. La primera es que el tamaño el grupo es pequeño, al ser solo siete personas, no hay una justificación para seleccionar una muestra más pequeña, ya que se puede acceder a la totalidad sin que ello aumente los costos o tiempos del estudio.

Otra razón es que los sistemas tributarios son operados exclusivamente por el equipo de TIC, ningún otro funcionario del GAD tiene el conocimiento técnico y operativo necesario para atender controles de acceso, gestión de incidentes, arquitectura de sistemas o vulnerabilidades tecnológicas; incluir a personas ajenas al área habría restado validez al diagnóstico.

Además, la investigación no busca generalizar sus hallazgos a otros municipios o instituciones, lo que se busca es comprender a fondo la realidad específica del GAD municipal del cantón Salcedo. Cada uno de los siete funcionarios aporta conocimientos sobre componentes específicos de los sistemas, como bases de datos, redes, desarrollo de software, atención a usuarios, entre otros, excluir a alguno de ellos implicaría perder una perspectiva necesaria para un diagnóstico integral. Debido al tipo de muestreo utilizado, censal y no probabilístico, los resultados obtenidos no son estadísticamente generalizables a otros GADs municipales, ya que cada institución tiene su propia realidad tecnológica, organizativa y presupuestaria, por lo que este estudio involucra directamente al GAD municipal del cantón Salcedo.

En cuanto al control del sesgo de deseabilidad social, y al ser una encuesta aplicada a funcionarios públicos que evalúa el nivel de cumplimiento de controles de seguridad, existe el

riesgo de que los participantes respondan de una manera socialmente aceptable, esto podría alterar el nivel real de implementación de los controles con el fin de no evidenciar debilidades institucionales o personales. Para minimizar este riesgo, se implementaron varias estrategias.

En primer lugar, entre las preguntas que contenía el cuestionario, se añadieron preguntas de carga del participante necesarias para organizar los resultados, pero cuya respuesta y el resultado de la misma no serían entregados a los superiores jerárquicos ni serán utilizados para evaluaciones del desempeño laboral. Cada encuestado fue identificado solamente con un código interno, que sólo conocí al investigador y que se presentó de forma agrupada y no a nivel de una única persona. En segundo lugar, se hizo saber a los encuestados que las respuestas que emitieron en la encuesta serían sólo utilizadas con fines académicos antes de su aplicación. En tercer lugar, el cuestionario fue diseñado con preguntas neutras y basadas en hechos concretos y no se formularon preguntas valorativas.

Finalmente, el diagnóstico obtenido con la encuesta se contrarresta con un análisis técnico independiente donde se incluye la entrevista con un especialista experto en la materia, la revisión de vulnerabilidades con la herramienta Wazuh y el análisis de las capturas de sistema tributario. Esta triangulación permitió identificar discrepancias entre la percepción reportada y el estado real de los sistemas. Gracias a estas medidas, se logró reducir el impacto del sesgo de deseabilidad social y aumentar la confiabilidad de los hallazgos.

2.2.4 IDENTIFICACIÓN DE ACTIVOS DE INFORMACIÓN

Como parte del proceso metodológico, se realizó la identificación general de los activos de información de la infraestructura tecnológica del Gobierno Autónomo Descentralizado Municipal

del Cantón Salcedo. Este inventario permitió definir los elementos críticos que sostienen los servicios de la institución: servidores, sistemas, bases de datos, redes de comunicación, etc.

La identificación de los activos se realizó con un enfoque general, tendiente a identificar a los elementos principales de la infraestructura tecnológica sin entrar en las configuraciones técnicas específicas, en función de su tipo, su nivel de criticidad y su papel dentro de los procesos institucionales que soportan los servicios que ofrece la institución en el ámbito tributario. Este inventario constituye la base del análisis de riesgos y la asignación de los resultados obtenidos a partir del uso de los instrumentos de recolección de datos.

La criticidad de los activos se logra a través de una evaluación cualitativa a partir de medir el impacto que tendría la afectación del activo en los aspectos de confidencialidad, integridad, disponibilidad de la información y continuidad de los servicios de la institución. Se asignaron críticas **altas** a los activos cuyo acceso no autorizado, pérdida, alteraciones e indisponibilidad podrían verse afectados, comprometiendo como información sensible, afectando procesos tributarios vitales para la institución o interrumpiendo los servicios de la institución. En cambio, se asignó criticidad **media** a los activos cuya afectación tendría un impacto operativo moderado, recuperable y con menor incidencia directa sobre los procesos estratégicos del GAD.

En base a este criterio, se considera que las asignaciones que corresponden a la categoría de servidores, bases de datos, sistemas, aplicaciones, red de datos e información institucional sean de alta criticidad, en razón de tener una relación directa con la gestión tributaria y con la protección de datos. Con carácter opuesto, los grupos de trabajo de usuario son considerados con nivel de criticidad media (en razón de que su afección, incluso en un único entorno de trabajo de usuario,

puede incidir en la operación habitual, pero no es capaz de poner en cuestión la continuidad de funcionamiento del servicio tributario).

Tabla 3. Inventario general de activos de información

ID	Activo	Tipo	Descripción	Responsable	Criticidad
A1	Servidores institucionales	Físico/Lógico	Equipos que alojan sistemas y servicios institucionales	TIC	Alta
A2	Sistema de recaudación tributaria	Software	Sistema que gestiona ingresos municipales	TIC / Financiero	Alta
A3	Base de datos institucional	Información	Almacena datos financieros, personales y administrativos	TIC	Alta
A4	Red institucional	Infraestructura	Conectividad interna y externa de la institución	TIC	Alta
A5	Equipos de usuario (estaciones de trabajo)	Físico	Computadores del personal institucional	TIC / Usuarios	Media
A6	Aplicaciones institucionales	Software	Sistemas administrativos y operativos	TIC	Alta
A7	Información institucional	Información	Datos personales, financieros y administrativos	Institución	Alta

Nota: Información de análisis institucional

2.2.5 PROCEDIMIENTO PARA LA RECOLECCIÓN Y ANÁLISIS DE DATOS

El procedimiento metodológico se desarrolla en varias etapas, en primer lugar, se realiza la revisión de literatura científica y normativa relacionada con la ciberseguridad, los estándares internacionales y la protección de datos personales, con el fin de sustentar teóricamente el estudio.

Posteriormente, se diseñan y validan los instrumentos de recolección de información, los cuales son aplicados al personal de la Jefatura de TIC y al experto en ciberseguridad.

Recopilados los datos, estos son procesados y analizados por medio de técnicas de análisis descriptivo, las que permiten identificar el nivel de cumplimiento de los controles de seguridad, las principales brechas existentes y los riesgos vinculados a los sistemas tributarios municipales. Finalmente, los resultados del análisis servirán de base para el diseño del plan de fortalecimiento de la ciberseguridad que se propone en el Capítulo III de este trabajo.

CAPÍTULO III

3. ANÁLISIS DE RESULTADOS

En este capítulo se presentan los resultados obtenidos a través de los instrumentos de recolección de información aplicados al personal de la Jefatura de Tecnologías de la Información y Comunicación (TIC) del Gobierno Autónomo Descentralizado Municipal del cantón Salcedo, los resultados se muestran en el Anexo C. El análisis integra los hallazgos cuantitativos derivados del cuestionario estructurado tipo Likert y los criterios cualitativos aportados por el experto en ciberseguridad entrevistado, mediante un proceso de triangulación metodológica orientado a caracterizar el estado actual de la ciberseguridad en los sistemas tributarios institucionales e identificar las brechas existentes.

3.1 CARACTERIZACIÓN DE LA MUESTRA

La población objeto de estudio estuvo conformada por los siete (7) servidores públicos que conforman la Jefatura de TIC del GAD municipal del cantón Salcedo, aplicándose un muestreo censal. Los datos sociodemográficos obtenidos se presentan en las siguientes tablas.

Tabla 4. Distribución del personal por cargo

Cargo / Función	Frecuencia	Porcentaje (%)
Analista	3	42.9
Analista de Desarrollo	1	14.3
Técnico de Soporte	2	28.6
Jefe de TIC	1	14.3
Total	**7**	**100.0**

Nota. Información a partir de los datos de la encuesta aplicada (2026).

La distribución por cargo indica que el 42.9% del personal corresponde a analistas, seguido de técnicos de soporte con el 28.6%. El jefe de TIC y el analista de desarrollo representan, respectivamente el 14.3% del total de participantes.

Tabla 5. Distribución del personal por tiempo de servicio y formación académica

Categoría	Frecuencia	Porcentaje (%)
Tiempo de servicio: Menos de 2 años	1	14.3
Tiempo de servicio: De 2 a 5 años	5	71.4
Tiempo de servicio: Más de 5 años	1	14.3
Formación académica: Ingeniería	7	100.0

Nota. Información a partir de los datos de la encuesta aplicada (2026).

El 71.4% del personal tiene entre 2 y 5 años de servicio en la institución, mientras que el 14.3% tiene menos de 2 años y el 14.3% restante más de 5 años. En cuanto a la formación académica, el 100% de los participantes posee título universitario en el área de ingeniería, lo que evidencia un equipo técnico con formación profesional homogénea en el ámbito de las tecnologías de la información.

3.2 RESULTADOS DEL CUESTIONARIO POR DIMENSIONES

A continuación, se presentan los resultados obtenidos en cada una de las cuatro secciones del cuestionario estructurado, organizado en torno a los dominios prioritarios de la ciberseguridad institucional. Para la interpretación de las medias aritméticas obtenidas en la escala Likert de 1 a 5, se utilizó el baremo que se muestra en la tabla 6, cuyos promedios se obtuvieron con el procedimiento de intervalos iguales sugerido por Hernández y Mendoza (2018), que establece rangos con una amplitud de 0.80.

Tabla 6. Baremo de interpretación de la escala Likert

Rango de Media	Percepción de implementación	Interpretación
1.00 – 1.80	Muy bajo	Ausencia total de controles
1.81 – 2.60	Bajo	Controles muy deficientes
2.61 – 3.40	Medio	Controles parcialmente implementados
3.41 – 4.20	Alto	Controles mayormente implementados
4.21 – 5.00	Muy alto	Controles plenamente implementados

Nota. Baremo construido siguiendo el método de intervalos iguales propuesto por Hernández y Mendoza (2018). Para una escala Likert de 5 puntos (valor mínimo = 1, valor máximo = 5), se calculó la amplitud del intervalo mediante la fórmula (máximo – mínimo) / número de categorías = (5 – 1) / 5 = 0.80. A partir del mínimo (1.00) se sumó sucesivamente 0.80 para obtener cada límite superior, ajustando el inicio de cada intervalo en 0.01 para evitar solapamiento (1.81, 2.61, etc.), excepto en el último intervalo que finaliza en 5.00.

3.2.1 SECCIÓN 1: GOBERNANZA Y POLÍTICAS DE SEGURIDAD

La primera sección evaluó el nivel de formalización, difusión y revisión de las políticas de seguridad de la información en la institución. Los resultados se detallan en la siguiente tabla.

Tabla 7. Resultados Sección 1: Gobernanza y Políticas de Seguridad

Ítem	Enunciado	1	2	3	4	5	Media
1	Existen políticas formales de seguridad de la información aprobadas y vigentes.	0	2	3	2	0	3.00
2	Las políticas son conocidas y difundidas entre el personal TIC.	0	1	5	1	0	3.00
3	Se realizan revisiones periódicas del cumplimiento de políticas y procedimientos.	0	0	5	2	0	3.29

Media de la sección	**3.10**

Nota. Escala: 1: Totalmente en desacuerdo; 5: Totalmente de acuerdo.

Los resultados de la primera sección presentan un cumplimiento medio en gobernanza y políticas de seguridad con una media global de 3.10. El ítem 1, que se refiere a la existencia de la política de seguridad formalmente aprobadas y vigentes, presentó una media de 3.0, con un 28.6% de los participantes en desacuerdo y un 42.9% en posición neutral, lo que hace pensar que las políticas existentes no se encuentran formalizadas y tampoco actualizadas; el ítem 2, que se refiere a la difusión de las políticas fue de 3.0, ya que a la vez se concentró el 71.4% de las respuestas en posición neutral; el ítem 3, sobre la revisión de período del cumplimiento, presentó la media más alta de la sección 3.29 aunque no se encuentra por encima del nivel medio. Estos resultados hacen percibir que debe hacerse un esfuerzo para mejorar los procesos de gobernanza de la seguridad de la información, especialmente en lo que se refiere a la formalización, socialización y revisión periódica de las políticas institucionales.

3.2.2 SECCIÓN 2: CONTROL DE ACCESO Y PROTECCIÓN DE LA INFORMACIÓN

La segunda sección evaluó el nivel de implementación de controles de acceso, gestión de permisos y protección de la información sensible de los contribuyentes. Los resultados se presentan en la Tabla 8.

Tabla 8. Resultados Sección 2: Control de Acceso y Protección de la Información

Ítem	Enunciado	1	2	3	4	5	Media
4	Los accesos se gestionan mediante credenciales personales asignadas a cada usuario.	0	0	3	4	0	3.57
5	Los accesos se conceden de acuerdo a la función y se revisan regularmente.	0	0	3	4	0	3.57
6	La información sensible se maneja de acuerdo a los principios de la integridad y de la confidencialidad.	0	0	1	6	0	3.86
Media de la sección						**3.67**	

Nota. Escala: 1:Totalmente en desacuerdo; 5:Totalmente de acuerdo.

En cuanto a la Sección 2, la puntuación que se obtuvo fue en promedio la más alta de las cuatro dimensiones que se está evaluando en la investigación, el valor fue de 3.67. Este resultado sugiere un alto nivel de cumplimiento. Pero, es importante señalar que esta calificación se refiere solamente a la percepción de los encuestados sobre la presencia de controles de acceso, sin considerar su efectividad o grado de funcionamiento.

Los ítems 4 y 5 encontraron su media en 3.57, siendo el 57.1% de los encuestados el que estaba de acuerdo o muy de acuerdo con las aseveraciones que formulaban estas afirmaciones. Sin embargo, un 42,9% se hallaba en una perspectiva neutral en ambas afirmaciones, de modo que, a pesar de que reconocen la existencia de los controles en acceso, no afirman la veracidad de su existencia o capacidad. El ítem 6, relativo a la gestión de información sensible en virtud de los principios de integridad y confidencialidad, fue el que mayores medios presentó en el cuestionario (3.86), siendo el 85.7% de los encuestados los que estaban de acuerdo con el enunciado. Este

resultado muestra una percepción favorable sobre la existencia de políticas de manejo de información sensible.

En conjunto, los resultados derivados del análisis muestran que los controles de acceso están establecidos bajo la forma de normas, pero los porcentajes de averiguaciones neutras también permiten evidenciar acciones de mejora que emergen en una revisión formal y periódica de los permisos de acceso por roles.

3.2.3 SECCIÓN 3: GESTIÓN DE INCIDENTES Y CONTINUIDAD OPERATIVA

La tercera sección evaluó la existencia de procedimientos documentados para la gestión de incidentes, la realización de respaldos y la disponibilidad de planes de continuidad operativa. Los resultados se presentan a continuación.

Tabla 9. Resultados Sección 3: Gestión de Incidentes y Continuidad Operativa

Ítem	Enunciado	1	2	3	4	5	Media
7	Existen procedimientos documentados para reportar y gestionar incidentes.	0	1	6	0	0	2.86
8	Los respaldos se almacenan en medios seguros y se realizan pruebas periódicas de recuperación.	0	0	0	5	2	4.29
9	La institución cuenta con mecanismos o planes de continuidad ante fallas o ataques.	0	0	5	2	0	3.29
Media de la sección						**3.48**	

Nota. Escala: 1: Totalmente en desacuerdo; 5: Totalmente de acuerdo.

La Sección 3 presentó resultados heterogéneos entre sus ítems. El ítem 8, correspondiente a la gestión de respaldos y pruebas de recuperación, fue el de mayor puntuación en todo el instrumento, con una media de 4.29 y el 100% de los participantes ubicados entre las valoraciones 4 y 5, lo cual refleja una práctica de resguardo de información bien establecida. El ítem número 7, centrado en la existencia de procedimientos documentados para la gestión de los incidentes, fue el que obtuvo la media más baja, 2.86 con un 85,7% de encuestados en posición neutral y un 14,3% en desacuerdo. Esto implica una brecha significativa por cuanto, no contar con procedimientos documentados redundará negativamente en la respuesta, en los incidentes y en la aplicación de las lecciones aprendidas. El ítem 9, que trataba sobre planes de continuidad operativa, quedó con un resultado medio de 3.29, de tal forma que se puede afirmar que los mecanismos de la continuidad se encuentran parcialmente implementados.

3.2.4 SECCIÓN 4: CAPACITACIÓN Y CULTURA DE CIBERSEGURIDAD

La cuarta sección evaluó el nivel de capacitación del personal técnico, la promoción de la concienciación institucional y el conocimiento de los procedimientos de respuesta ante amenazas.

Tabla 10. Resultados Sección 4: Capacitación y cultura de ciberseguridad

Ítem	Enunciado	1	2	3	4	5	Media
10	El personal técnico recibe capacitaciones periódicas sobre ciberseguridad.	0	0	6	1	0	3.14
11	Se promueve la concienciación del personal respecto a la protección de la información.	0	0	5	1	1	3.43

12	El personal conoce los pasos a seguir ante una amenaza o vulnerabilidad detectada.	0	2	4	0	1	3.00
Media de la sección						**3.19**	

Nota. Escala: 1: Totalmente en desacuerdo; 5: Totalmente de acuerdo.

La Sección 4 obtuvo un promedio de 3.19, ocupando una posición en el nivel medio. El ítem 11, que trata sobre fomentar la concienciación del personal, logró la puntuación más elevada dentro de la sección 3.43 (nivel alto), aunque se identifica una dispersión moderada, ya que el 71.4% de las posiciones era "neutral". En cuanto a la frecuencia con que las capacitaciones de ciberseguridad son impartidas (ítem 10), se detecta una media de 3.14, dado que el 85.7% de las respuestas posiciona "neutral ", lo que pone de manifiesto que, aunque el personal reconoce que tiene actividades formativas, éstas tienen lugar de un modo no sistemático, ni regulador. Con respecto a los procedimientos de respuesta ante amenazas (ítem 12), esta consideración alcanzó el valor promedio de 3.00, con un 28.6 % en desacuerdo, lo cual da cuenta de una brecha relevante en la cultura de ciberseguridad institucional.

3.3 RESUMEN GENERAL DE RESULTADOS POR DIMENSIÓN

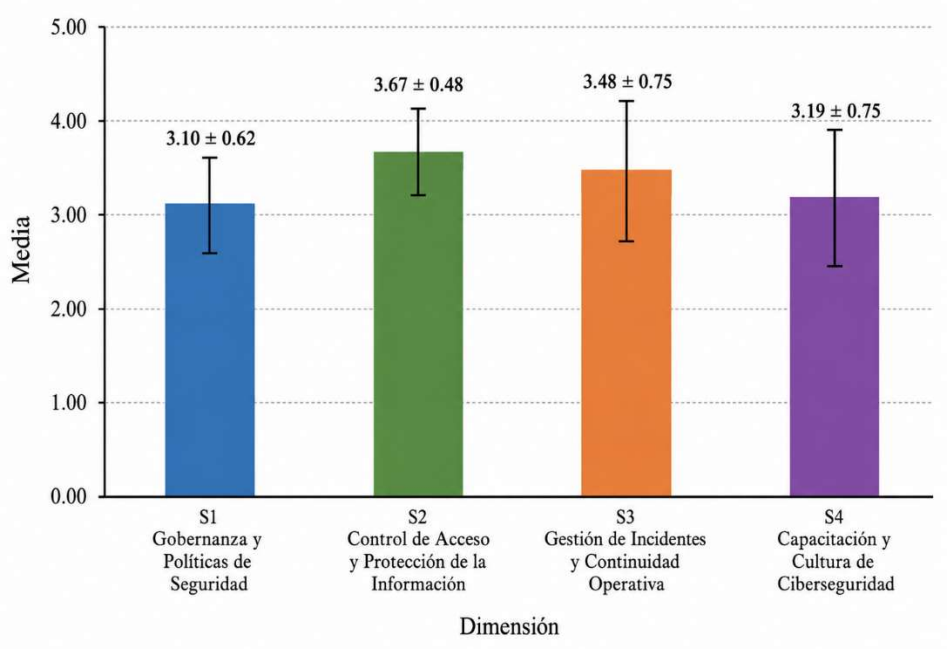
La Tabla 11 consolida los resultados obtenidos en las cuatro dimensiones evaluadas, permitiendo una visión comparativa del estado de la ciberseguridad en los sistemas tributarios del GAD municipal del cantón Salcedo.

Tabla 11. Resumen de medias por dimensión y percepción de implementación

Dimensión	Media	Desviación estándar	Percepción de implementación
S1: Gobernanza y Políticas de Seguridad	3.10	0.62	Medio
S2: Control de Acceso y Protección	3.67	0.48	Alto
S3: Gestión de Incidentes y Continuidad	3.48	0.75	Alto
S4: Capacitación y Cultura de Ciberseguridad	3.19	0.75	Medio
Media General	**3.36**	**0.69**	**Medio**

Nota. Información a partir de los datos de la encuesta aplicada al personal TIC del GAD Municipal del cantón Salcedo (2026), la desviación estándar indica la dispersión de las respuestas.

Figura 2. Comparación de medias por dimensión



Nota: La figura muestra las medias por dimensión y su respectiva dispersión mediante la desviación estándar.

Los resultados globales del cuestionario arrojan una media general de 3.36 sobre 5, la cual representa un nivel medio de percepción de los controles y prácticas de ciberseguridad de los sistemas tributarios institucionales. Las dimensiones más robustas son control de acceso y protección de la información (3.67) y gestión de incidentes y continuidad operativa (3.48) las cuales están situadas en niveles altos, si bien la calificación general varía en función de ítems específicos que evidencian debilidades relevantes, como, por ejemplo, la ausencia de procedimientos documentados para la gestión de incidentes (ítem 7, media = 2.86). Las dimensiones de gobernanza y políticas de la seguridad (3.10) y capacitación y cultura de la ciberseguridad (3.19) se sitúan en un nivel medio, evidenciando así ámbitos de intervención priorizados.

La desviación estándar fue calculada con las frecuencias agrupadas que fueron el resultado de cada dimensión, considerando los valores de la escala de Likert de 1 a 5, y el total de respuestas acumuladas por sección. Cada sección estuvo integrada por tres ítems aplicados a siete participantes, por lo que se consideraron 21 respuestas por sección, permitiendo identificar el grado de dispersión de las valoraciones respecto a la media de cada dimensión.

Al observar la desviación estándar presentada en la Tabla 11 se puede comprobar que la dimensión de Control de Acceso (0.48) tiene menor dispersión, por lo que hay un gran grado de acuerdo entre los siete encuestados. Le sigue en mayor dispersión la dimensión de Gobernanza (0.62), también con dispersión baja. Al contrario, Gestión de Incidentes y Capacitación (ambos con 0.75) tienen dispersión moderada, por lo que se puede observar que hay opiniones más divididas. Es decir, hay técnicos de procedimientos que tienen la intuición de que hay documentos que otorgan instrucciones para atender incidentes o que asisten a capacitaciones periódicas, pero

también existen técnicos que entienden que eso no es suficiente o que no hay dichos documentos en las organizaciones. La carencia de consenso es un hallazgo que se considera importante, pues pone de manifiesto que hay prácticas en estas dos áreas que no están estandarizadas y no son vistos también en el mismo sentido por el equipo, a diferencia de la mayor uniformidad de criterio en Control de Acceso y Gobernanza.

3.4 RESULTADOS DE LA ENTREVISTA AL EXPERTO EN CIBERSEGURIDAD

Como parte del componente cualitativo de la investigación, se añadió el punto de vista de un experto en ciberseguridad. A diferencia de la encuesta que siguió un criterio estadístico, para la entrevista fue seleccionado un experto por su conocimiento y experiencia en el tema.

Para la selección del experto se buscó a un profesional con amplia trayectoria en implementación de estándares internacionales de seguridad y gestión de riesgos en el sector público ecuatoriano. En la institución la persona con dicha experiencia ocupa el cargo de jefe de Tecnologías de la Información y Comunicación, quién conoce sobre la evaluación y mejora de la ciberseguridad en entidades públicas; y tiene competencias relacionadas con la tecnología que está aplicada en los sistemas tributarios.

Esto se debe a que su perfil muestra que sus observaciones se basan en hechos reales, en lugar de opiniones vagas, reflejando de esta manera la realidad que existe en los gobiernos locales en en país. Con la aplicación de la entrevista se pudo validar y complementar los hallazgos cuantitativos que se obtuvieron al aplicar el cuestionario, desde un enfoque técnico especializado. Los resultados están organizados por temas.

El jefe de TIC identificó que entre los principales problemas identificados es la falta de un Sistema de Gestión de Seguridad de la Información (SGSI), lo que implica que las instituciones municipales en Ecuador operen con controles aislados de seguridad, y cuyo resultado sea la fata de una política unificada en materia de seguridad. Esta información se ajusta a la información obtenida en la Sección 1 del cuestionario, donde las políticas formales y su difusión, no alcanzaron los promedios de las medias de los ítems relacionados.

Con relación al control de accesos, indicó que, la asignación de credenciales personales es un control básico que se está cumpliendo, sin embargo, la gestión de los privilegios privilegiados y la revisión periódica de los permisos son debilidades significativas presentes en los sistemas desarrollados en tecnologías obsoletas, como el PHP que no tiene soporte activo, y que están presentes en el GAD. Indicó que el principio de mínimo privilegio, el cual es recogido en la ISO/IEC 27001:2022 como en la NIST CSF, suele ser ignorado en organizaciones con baja madurez en ciberseguridad.

Entorno a la gestión de los incidentes, el experto indicó que la no formalización de procedimientos para la detección, clasificación y respuesta de los incidentes de seguridad es uno de los riesgos más importantes porque ante la falta de un procedimiento las organizaciones no garantizan tiempos de respuesta adecuados ni la trazabilidad necesaria para realizar posteriores análisis forenses. Tal hallazgo coincide con el ítem 7 del cuestionario, que obtuvo la media más baja del mismo.

Por último, el experto observa que la formación en ciberseguridad no solo ha de estar destinada para el personal técnico, sino también para todos los funcionarios que manipulan los sistemas de información, haciendo especial hincapié en la detección de amenazas como las del tipo

phishing, del tipo ingeniería social y el uso incorrecto de las claves de acceso. Aconsejó la disposición de programas de concienciación con una frecuencia al menos semestral en relación con la puesta en práctica de los principios de la norma ISO/IEC 27001:2022 y las mejores prácticas del NIST CSF. Los resultados están expuestos en el Anexo E.

3.5 EVIDENCIA TÉCNICA COMPLEMENTARIA

Con el propósito de complementar y validar los hallazgos obtenidos mediante la encuesta y la entrevista al experto, se incorpora evidencia técnica documental obtenida del sistema de monitoreo de seguridad Wazuh y de capturas de pantalla de los sistemas tributarios en operación. Esta evidencia no constituye la base del diagnóstico, sino que corrobora objetivamente las debilidades reportadas por el personal TIC y permite ilustrar de manera concreta las brechas identificadas.

3.5.1 USO DE HERRAMIENTA DE MONITOREO DE SEGURIDAD

El análisis con la herramienta Wazuh permitió identificar un total de 3.352 vulnerabilidades en el servidor llamado "*servidorweb191*", distribuidas en los paquetes de software del sistema operativo y aplicaciones instaladas. Es importante puntualizar dos aspectos que se relacionan con este hallazgo: el primero es que esta cifra se refiere únicamente a este servidor, ya que no se ha evaluado el resto de la infraestructura del GAD; y segundo, el hecho de que se encuentre una vulnerabilidad no implica que necesariamente sea explotable, sino que implica que existe una exposición potencial que, en combinación con otras debilidades, podría elevar el riesgo. El análisis estaba limitado al servidor "servidorweb191", y principalmente por dos razones: Primera, por ser el activo más crítico de la infraestructura, dado que sistematiza los sistemas de recaudación tributaria que sustentan los ingresos públicos del cantón. Segunda, porque el objetivo de este

análisis técnico no era un inventario de vulnerabilidades de toda la red, si no contrastar, a través de evidencia objetiva, que las debilidades referidas por el personal TIC en la encuesta tienen consistencia real. En el Anexo F hay un extracto de referencia del informe de vulnerabilidades detectadas por la herramienta Wazuh.

Tabla 12. Distribución de vulnerabilidades por nivel de severidad

Severidad	Cantidad	Porcentaje
Crítica	3	0.09%
Alta	1.659	49.49%
Media	75	2.24%
Baja	1.579	47.10%
Desconocida	36	1.07%
Total	**3.352**	**100%**

Nota: Fuente: Reporte de vulnerabilidades generado por Wazuh

Tabla 13. Distribución de vulnerabilidades por año de publicación (CVE)

Año	Cantidad	Porcentaje
2023	18	0.54%
2024	741	22.11%
2025	2.554	76.19%
2026	39	1.16%
Total	**3.352**	**100%**

Nota: Fuente: Reporte de vulnerabilidades generado por Wazuh

Los resultados evidencian que el servidor presenta una alta exposición a vulnerabilidades de severidad Alta (49.49%), muchas de ellas correspondientes a fallas publicadas en 2025 (76.19%), lo que indica una falta de aplicación oportuna de parches de seguridad. Este descubrimiento da sostenimiento a la brecha de infraestructura tecnológica y da argumentación a

la necesidad de llevar a cabo la ejecución de las acciones que se expondrán en el plan de fortalecimiento.

Cabe señalar que el informe de Wazuh no lleva incorporada explícitamente información acerca de la existencia de parches para cada vulnerabilidad, y esto responde al hecho de que, en muchas ocasiones vulnerabilidades afectan a componentes que no tienen soporte activo, ya que son versiones obsoletas de software. En este sentido, no se dispondría de parches, y la solución pasaría por complementar las medidas de seguridad con estrategia como segmentación, restricción de accesos, endurecimiento del sistema y monitoreo y vigilancia permanente. Por otro lado, las vulnerabilidades de componentes que aún tienen soporte se pueden solucionar con una buena gestión de actualizaciones. Esto muestra que hay debilidades en cómo se gestionan los parches en la infraestructura analizada.

3.5.2 EVIDENCIA DE CONFIGURACIÓN Y OPERACIÓN DE LOS SISTEMAS TRIBUTARIOS

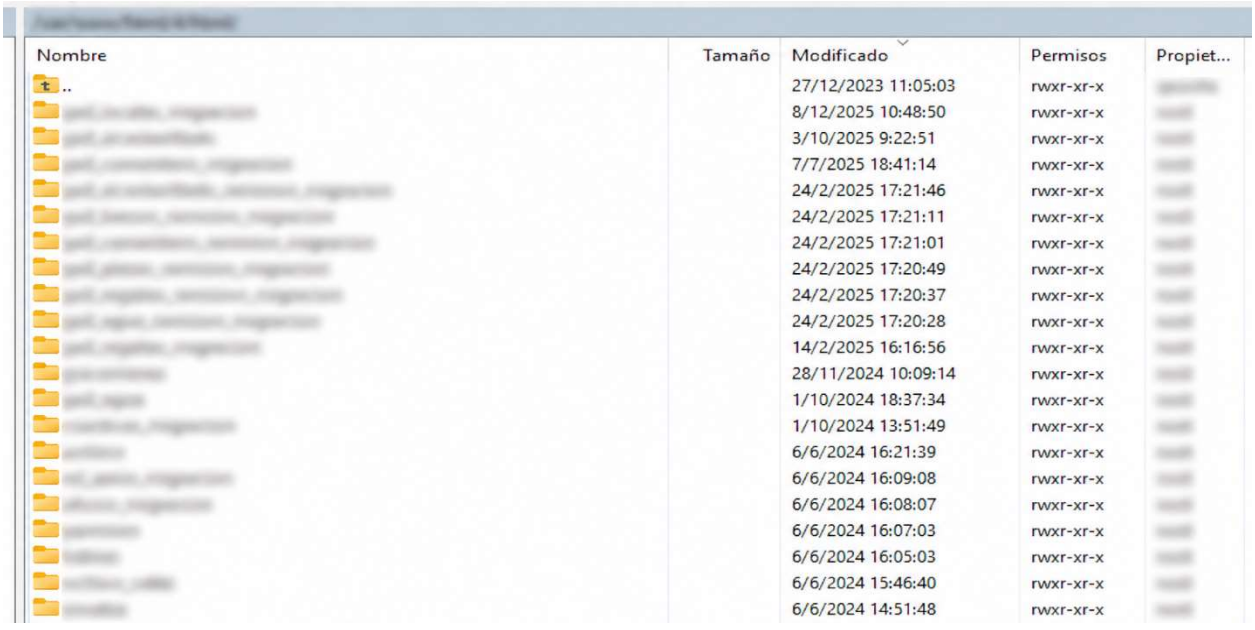
Con el propósito de ilustrar las condiciones técnicas actuales en las que operan los sistemas tributarios desarrollados internamente por el GAD municipal del cantón Salcedo, se presentan a continuación capturas de pantalla obtenidas en entornos controlados bajo ambientes de prueba y desarrollo, con el fin de cumplir con los principios de confidencialidad establecidos en la LOPDP. Adicionalmente se anonimizaron los datos sensibles que pudieran aparecer en las imágenes, tales como nombres de contribuyentes, números de identificación personal, valores específicos de transacciones o credenciales de acceso. Cabe mencionar que estas evidencias permitieron visualizar de manera tangible las debilidades identificadas en el diagnóstico institucional,

constituyéndose en un respaldo técnico cualitativo que complementa los resultados obtenidos a partir del instrumento de encuesta.

Es conveniente destacar que estas evidencias han permitido ratificar la confirmación de que existen vulnerabilidades sociotécnicas implicadas con el desarrollo de software, la gestión de bases de datos y el control de accesos en los sistemas tributarios. Las capturas que se presentan a continuación, se amparan en el anexo G, en el cual se encuentra la autorización otorgada por el GAD Municipal del cantón Salcedo, sobre la autorización del uso de información con fines de índole académica; garantizando que la recopilación de la misma no comprometa su confidencialidad, integridad, y disponibilidad de la información, en una intención de cumplir los principios de ética de la investigación y las normas vigentes en protección de datos.

3.5.2.1 ENTORNO DE DESARROLLO

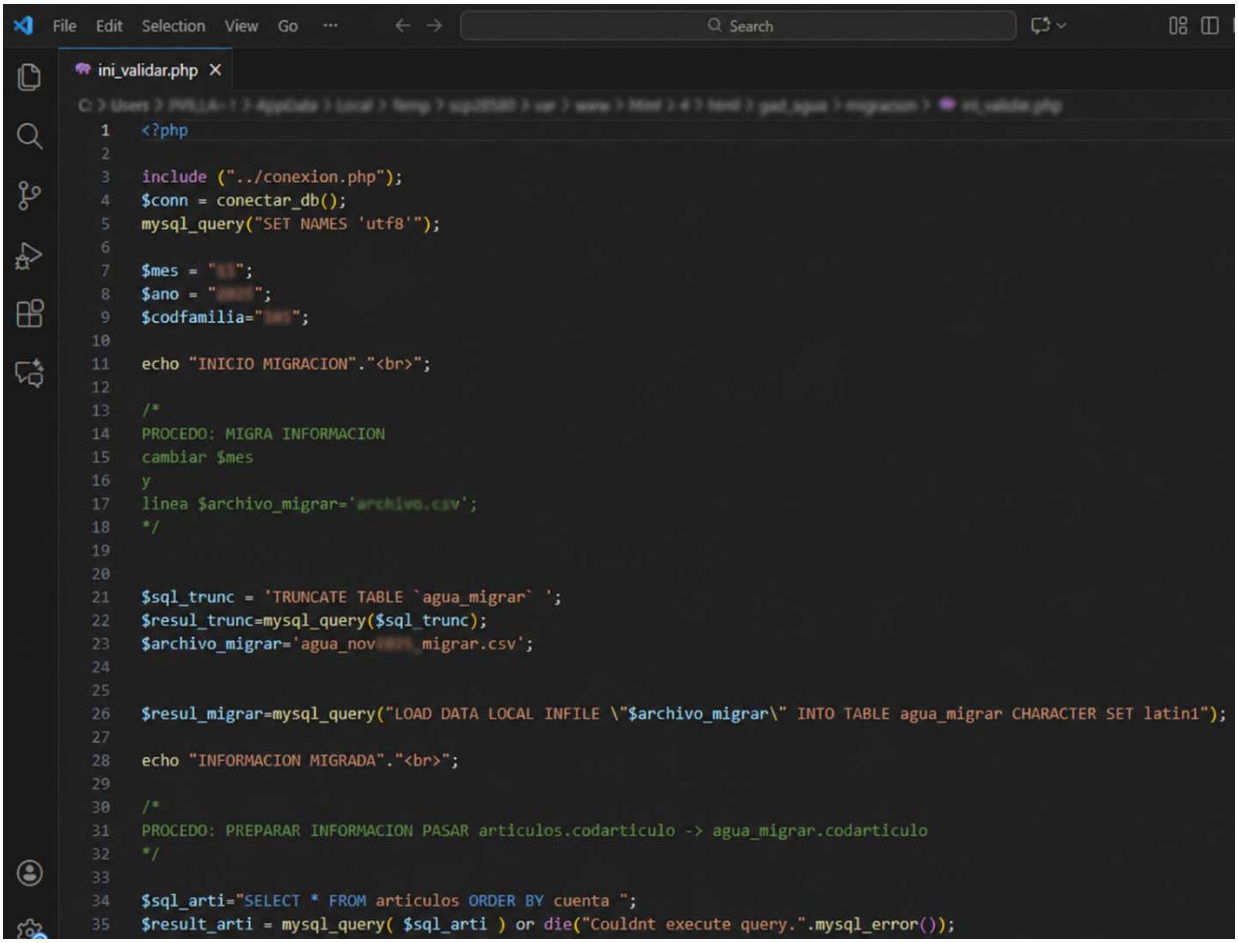
Figura 3. Archivos ejecutables del sistema



Nota: Fuente: La captura de esta imagen fue tomada desde el entorno de desarrollo, para protección de los datos contenidos en la misma, estos se han anonimizados.

En esta imagen se puede evidenciar que se accedió a los archivos ejecutables de los sistemas tributarios sin ninguna restricción o medidad de seguridad, puediendo ser facilmente modificables dichos archivos por los usuarios con permisos. Evidenciando que la forma de acceder a esta información presenta una vulnerabilidad crítica para la protección del código fuente, poniendo en riesgo a los sistemas.

Figura 4. Acceso al código fuente



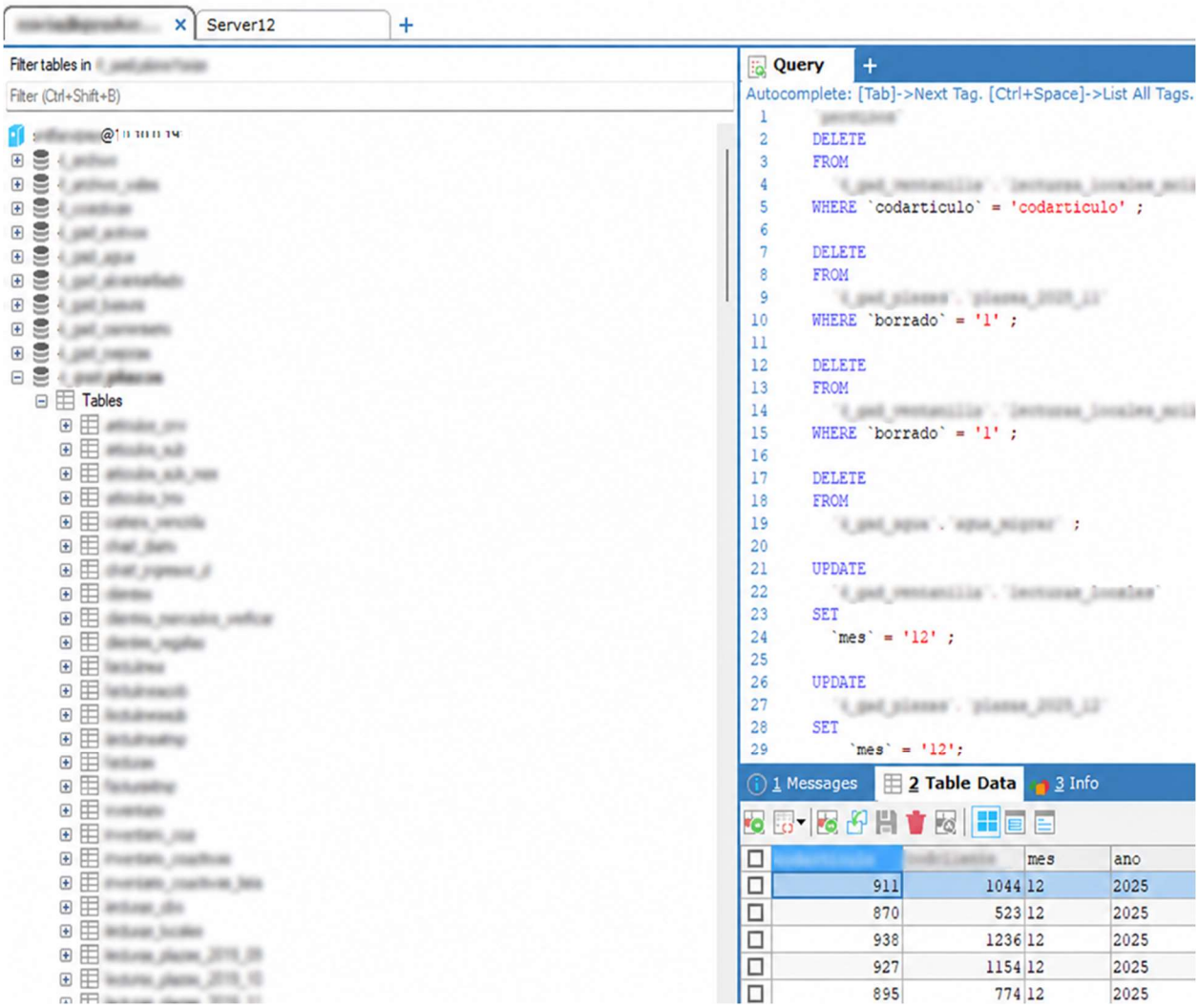
Nota: Fuente: Captura de imagen entorno de desarrollo, los datos sensibles fueron anonimizados

Se observa la utilización de funciones mysql_query que pertenecen a la extensión mysql de PHP, actualmente obsoleta y eliminada en versiones recientes del lenguaje, lo que hace

evidenciar el uso de tecnologías obsoletas para el desarrollo del sistema; y se puede observar la utilización de sentencias que permiten la carga directa de archivos hacia la base de datos sin evidencia de validar previamente el contenido de los mismos, con las implicaciones que conlleva un potencial de inyección de datos maliciosos o manipulación de la información.

3.5.2.2 BASES DE DATOS

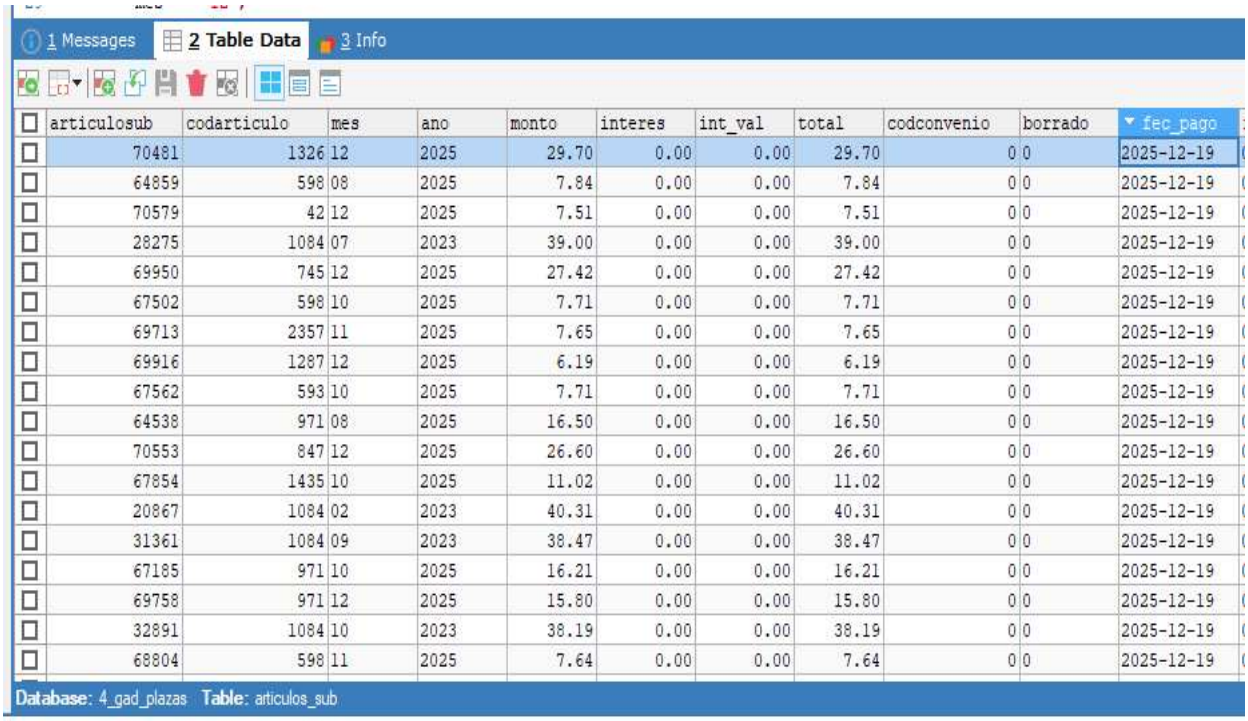
Figura 5. Acceso total a bases de datos



Nota: Fuente: Captura de imagen entorno base de datos, los datos sensibles fueron anonimizados

Se pone de manifiesto el acceso al gestor de la base de datos, en el que se observa como un usuario puede tener control sobre diferentes bases de datos referentes a distintos sistemas tributarios, lo que evidencia el incumplimiento del principio de mínimo privilegio ya que no se aprecia en esta herramienta segmentación y control de accesos diferenciados.

Figura 6. Manipulación directa de la información



1 Messages | 2 Table Data | 3 Info

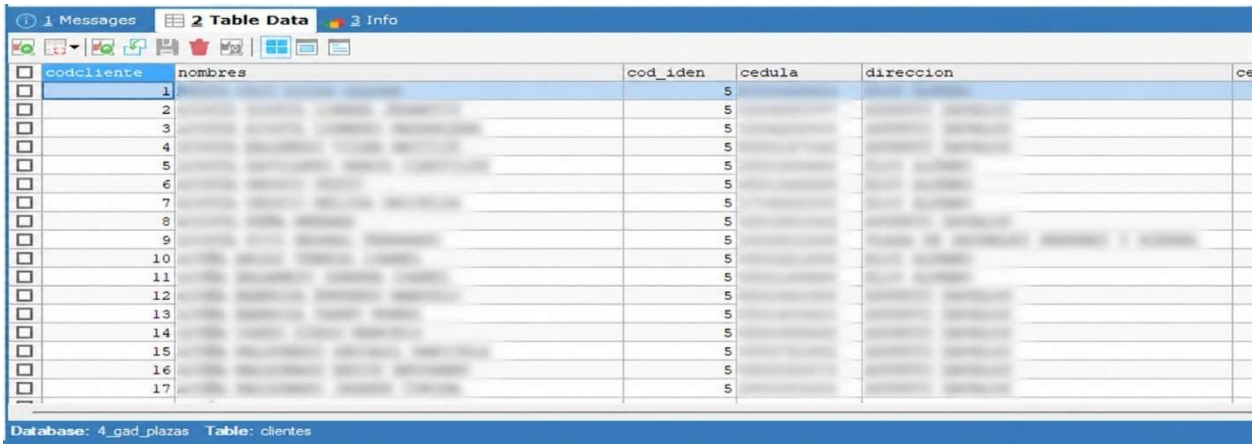
articulosub	codarticulo	mes	ano	monto	interes	int_val	total	codconvenio	borrado	fec_pago
70481	1326	12	2025	29.70	0.00	0.00	29.70	0	0	2025-12-19
64859	598	08	2025	7.84	0.00	0.00	7.84	0	0	2025-12-19
70579	42	12	2025	7.51	0.00	0.00	7.51	0	0	2025-12-19
28275	1084	07	2023	39.00	0.00	0.00	39.00	0	0	2025-12-19
69950	745	12	2025	27.42	0.00	0.00	27.42	0	0	2025-12-19
67502	598	10	2025	7.71	0.00	0.00	7.71	0	0	2025-12-19
69713	2357	11	2025	7.65	0.00	0.00	7.65	0	0	2025-12-19
69916	1287	12	2025	6.19	0.00	0.00	6.19	0	0	2025-12-19
67562	593	10	2025	7.71	0.00	0.00	7.71	0	0	2025-12-19
64538	971	08	2025	16.50	0.00	0.00	16.50	0	0	2025-12-19
70553	847	12	2025	26.60	0.00	0.00	26.60	0	0	2025-12-19
67854	1435	10	2025	11.02	0.00	0.00	11.02	0	0	2025-12-19
20867	1084	02	2023	40.31	0.00	0.00	40.31	0	0	2025-12-19
31361	1084	09	2023	38.47	0.00	0.00	38.47	0	0	2025-12-19
67185	971	10	2025	16.21	0.00	0.00	16.21	0	0	2025-12-19
69758	971	12	2025	15.80	0.00	0.00	15.80	0	0	2025-12-19
32891	1084	10	2023	38.19	0.00	0.00	38.19	0	0	2025-12-19
68804	598	11	2025	7.64	0.00	0.00	7.64	0	0	2025-12-19

Database: 4_gad_plazas Table: articulos_sub

Nota: Fuente: Captura de imagen entorno base de datos, los datos sensibles fueron anonimizados

Se observa que los valores que se relacionan con la recaudación tributaria pueden alterarse directamente en la base de datos, incluidos, por ejemplo, las cifras económicas o micrométricas o las importaciones, las fechas de pago y los registros históricos. Esta capacidad de modificación transgrediendo controles o validación supone una amenaza crítica de alterar la información contable.

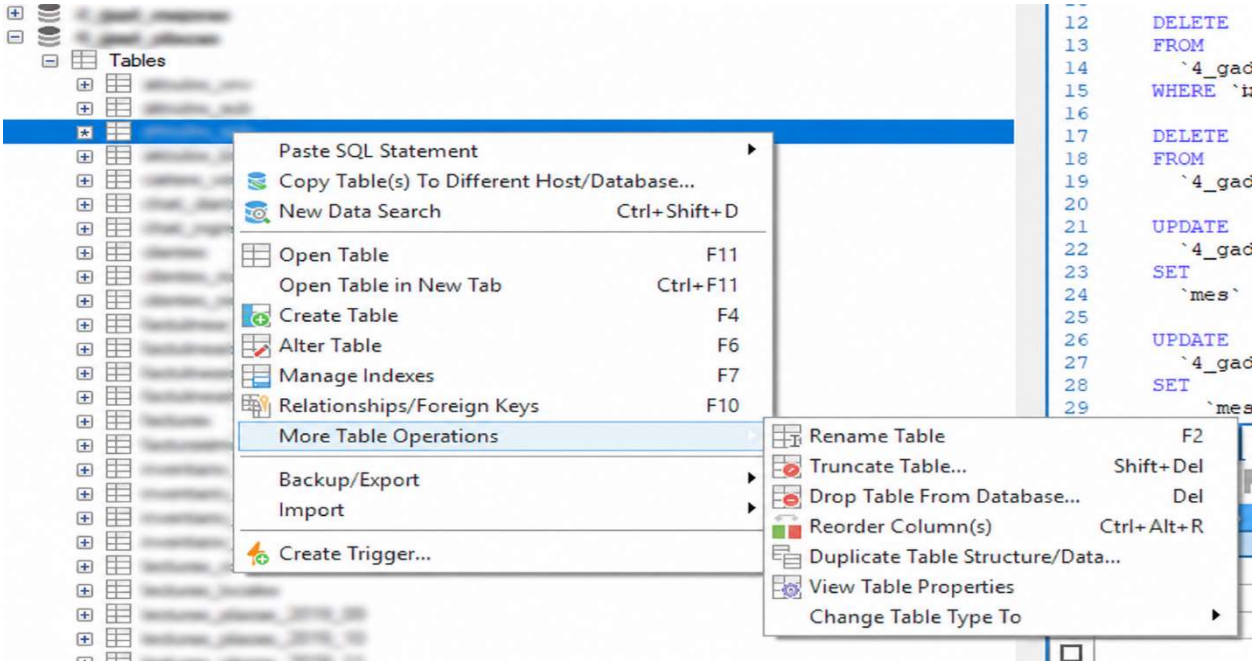
Figura 7. Acceso a datos personales sin protección



Nota: Fuente: Captura de imagen entorno base de datos, los datos sensibles fueron anonimizados

La captura expone el acceso directo a conocimiento de los contribuyentes (información de carácter personal y financiero) que existe en la base de datos, observándose que la misma no utiliza mecanismos de encriptación ni restricciones de acceso, contradiciendo así principios como el de confidencialidad o la norma de protección de los datos personales.

Figura 8. Ausencia de control de auditoría en bases de datos



Nota: Fuente: Captura de imagen entorno base de datos, los datos sensibles fueron anonimizados

Se constata que no existen registros de auditoría que permitan seguir la pista a las operaciones que se realizaron sobre las bases de datos, dado que no permite saber que usuario llevó a cabo modificaciones, eliminaciones o inserciones de información.

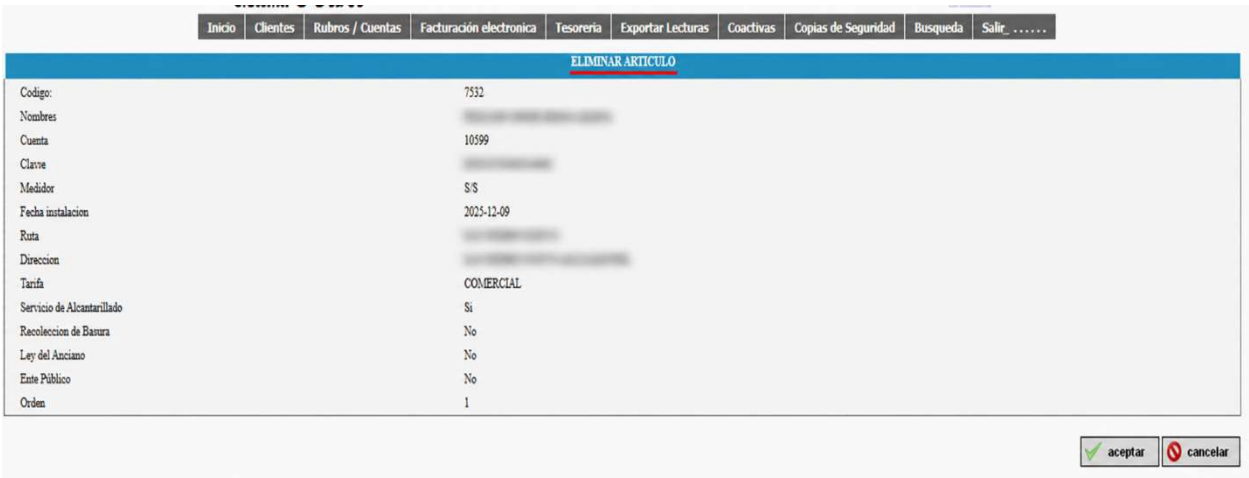
3.5.2.3 INTEFAZ DE SISTEMAS

Figura 9. Acceso total de usuarios sin restricción de roles

Nota: Fuente: Captura de imagen interfaz de sistemas, los datos sensibles fueron anonimizados

Se evidencia que los usuarios con determinados niveles de acceso (por ejemplo, nivel 9) pueden acceder a todos los módulos del sistema, independientemente de sus funciones, lo que demuestra la inexistencia de una adecuada separación de roles y privilegios.

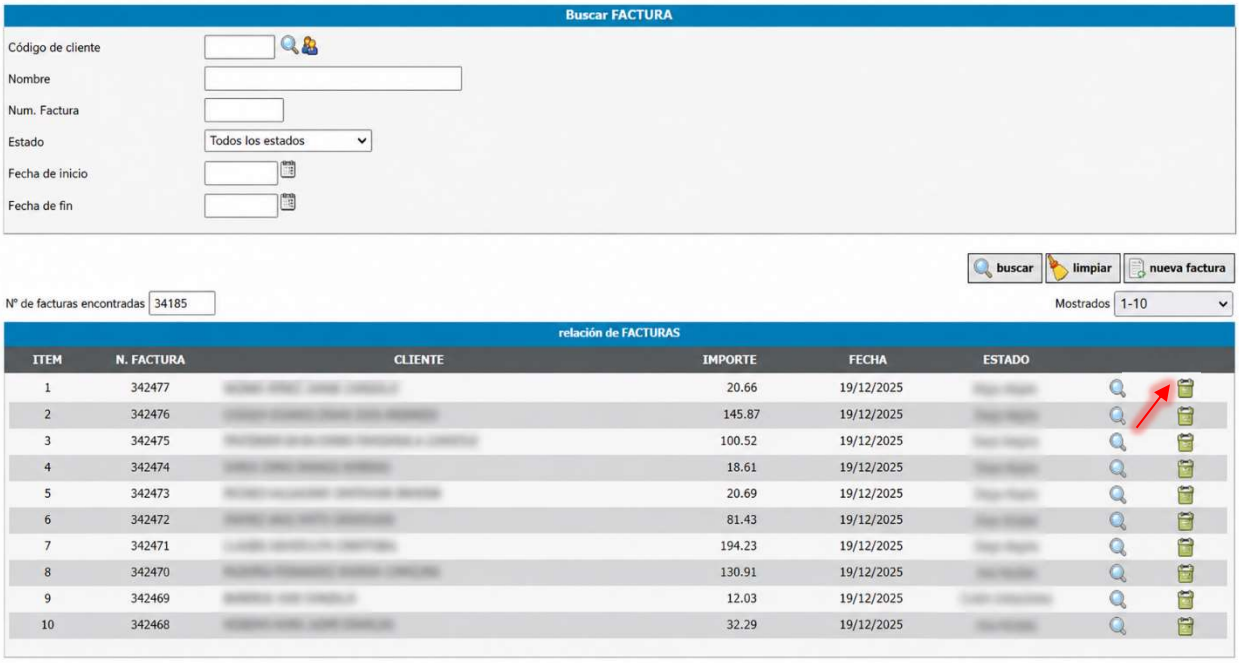
Figura 10. Eliminación de registros sin control



Nota: Fuente: Captura de imagen interfaz de sistemas, los datos sensibles fueron anonimizados

Se comprueba que los registros pueden eliminarse fácilmente, afectando incluso historiales de pago, no existen mecanismos de validación ni registro de auditoría, afectando la integridad de la información.

Figura 11. Eliminación de facturas sin trazabilidad



Nota: Fuente: Captura de imagen interfaz de sistemas, los datos sensibles fueron anonimizados

En el módulo de facturación se identifica la posibilidad de eliminar facturas ya cobradas sin que el sistema registre qué usuario realizó la acción, evidenciando la ausencia de controles de auditoría y trazabilidad.

3.5.2.4 ANÁLISIS

Las evidencias presentadas permiten confirmar, desde una perspectiva técnica, las debilidades identificadas en el diagnóstico institucional, particularmente en lo referente a la falta de controles de acceso, ausencia de mecanismos de auditoría, deficiencias en el desarrollo seguro de software y vulnerabilidades en la gestión de bases de datos. Estos resultados concuerdan con

los datos que la encuesta aplicada al personal de TIC ha proporcionado, los cuales muestran la percepción de deficiencias en controles de seguridad implementados. En este caso, los pantallazos constituyen un soporte empírico que hace constar las debilidades en la ciberseguridad de los sistemas tributarios, y dan cuenta de la necesidad de implementar políticas de seguridad en concordancia con estándares internacionales , como son la ISO/IEC 27001, el NIST Cybersecurity Framework y la normativa ecuatoriana.

Estas evidencias de igual manera como los registros de Wazuh, no constituyen la fuente principal de análisis, sino un elemento de validación que permite corroborar la existencia de vulnerabilidades.

3.6 ANÁLISIS DE BRECHAS DE CIBERSEGURIDAD

Se basó en la triangulación de los resultados, que fueron cuantitativos y cualitativos, y con la norma ISO/IEC 27001:2022 y el NIST CSF se identificaron brechas de ciberseguridad en los sistemas tributarios del GAD Municipal del cantón Salcedo. Estas debilidades, especialmente las que se relacionan con la gestión de incidentes, el control de accesos y la auditoría, dificultan el cumplimiento de la LOPDP, ya que incrementan los riesgos de acceder sin permisos e interrupen el seguimiento de las operaciones.

A continuación se presentan los criterios para evaluar las brechas:

Probabilidad (P):

1: Baja (eventos poco frecuentes, controles existentes.)

2: Media (ocurrencia posible, controles parciales.)

3: Alta (ocurrencia frecuente, procesos en ejecución. Ejemplo: varios CVE sin resolución.)

Impacto (I):

1: Bajo (afecta áreas no críticas.)

2: Medio (afecta procesos operativos.)

3: Alto (afecta servicios críticos, datos sensibles o continuidad.)

Fórmula:

Riesgo = Probabilidad * Impacto

Para evaluar el riesgo, se adoptó un enfoque cualitativo donde se verificó la probabilidad de que ocurra un evento y como impactaría a la institución. Para este análisis se adoptó una matriz de riesgos con tres categorías. La frecuencia y la cantidad de vulnerabilidades que se encontraron en la herramienta Wazuh, permitieron evaluar la probabilidad.

Para clasificar a cada dominio, con un nivel de probabilidad bajo (1), medio (2) o alto (3), se aplicó los siguientes criterios:

Probabilidad baja (1): Se considera que un dominio tiene una probabilidad baja cuando no se identifican vulnerabilidades críticas o significativas y cuando los controles documentados son suficientes para mitigar el riesgo. En el presente análisis no se asignaron dominios con probabilidad baja, debido a que los resultados evidenciaron brechas activas o controles parciales en todos los componentes evaluados.

Probabilidad media (2): Se hallaron brechas de nivel medio o bajo, no se vio que estén siendo aprovechadas activamente, pero hay partes que necesitan una mejora. Esta posibilidad se dio al ámbito de Gobernanza ya que se sabía de algunas reglas o hábitos institucionales, no obstante, los números de la encuesta muestran un grado intermedio de acatamiento en lo tocante a

formalizar, divulgar y repasar las directrices de seguridad. De igual manera que el dominio de Control de Acceso, este dominio es consciente de la existencia de mecanismos básicos que hacen uso de credenciales y una asignación de permisos; a pesar de ello, la existencia de respuestas neutrales y la falta de evidencias de revisiones periódicas nos indican que los controles no están del todo consolidados. En lo que respecta a Continuidad Operativa, sí se encuentran los mecanismos de respaldo, pero la existencia de planes de continuidad y recuperación requieren incrementar las acciones de formalización. Finalmente, la Capacitación porque se evidencian acciones de concienciación o formación, pero estas no se perciben como periódicas, sistemáticas ni plenamente institucionalizadas.

Probabilidad alta (3): Indicios claros de la existencia de vulnerabilidades graves o críticas en elementos esenciales, ausencia de parches disponibles, u obsolescencia del software. Esta probabilidad fue asignada a los dominios de Infraestructura Tecnológica, por presencia de vulnerabilidades de severidad alta y crítica detectadas por Wazuh, esta situación reflejó una exposición asociada a componentes tecnológicos que requieren actualización, endurecimiento o remediación. En Gestión de Incidentes, porque, aunque pueden existir prácticas informales de atención, los resultados muestran debilidad en la documentación de procedimientos para reportar, clasificar y responder ante incidentes, esto incrementa la posibilidad de que un evento de seguridad no sea gestionado oportunamente. De igual manera, Auditoría y Trazabilidad debido a la ausencia o debilidad de mecanismos formales de registro, seguimiento y revisión de eventos, lo que limita la capacidad institucional para detectar accesos no autorizados y demostrar trazabilidad sobre las operaciones realizadas en los sistemas tributarios.

En lo que respeta a la consideración al impacto evidenciada, se puso de manifiesto la posible afectación tanto de la confidencialidad como de la integridad y de la disponibilidad de la información y de la continuidad de los servicios institucionales. Por lo que los dominios relacionados con los datos sensibles de los contribuyentes, el funcionamiento de los sistemas tributarios, la respuesta ante los incidentes, la infraestructura crítica y la trazabilidad sufrieron un impacto alto (3), dado que la falta de funcionamiento de estos componentes podría afectar la información institucional, los servicios prestados o tener connotaciones legales en lo que hace a la protección de los datos personales. En cambio, Capacitación recibió una valoración de impacto medio 2, ya que su efecto es indirecto y se manifiesta de manera gradual; sin embargo, tiene una influencia significativa en la cultura de seguridad y en mitigación de incidentes.

Tabla 14. Matriz de evaluación de riesgos

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

Nota**:** La matriz de riesgos se elabora combinando los niveles de probabilidad e impacto, siendo el valor resultante el que establece la categorización del riesgo como bajo, medio, alto o crítico.

Sobre la base de esta serie de criterios, la clasificación vigente en la Tabla 15 presenta una buena fundamentación para la priorización de las brechas que se encuentran en la parte inferior, ya que los dominios Gestión de Incidentes, Infraestructura Tecnológica y Auditoría y Trazabilidad pueden calificarse de críticos, debido a que contienen altos niveles de impacto combinados con altos niveles de probabilidad. Esta evaluación tiene sentido, e incluso puede sustentarse con la

entrega de la evidencia ya que estos casos limitan las condiciones que pueden facilitar la aparición de incidentes y dificultar su detección, así como limitar la respuesta institucional e impide la recuperación de los incidentes. Por lo tanto, estas brechas deben abordadas de forma prioritaria en el Plan de Fortalecimiento de Ciberseguridad.

Tabla 15. Clasificación de brechas según matriz de riesgos

Dominio	Probabilidad	Impacto	Nivel de Riesgo
Gobernanza	2	3	**Alto (6)**
Control de Acceso	2	3	**Alto (6)**
Gestión de Incidentes	3	3	**Crítico (9)**
Continuidad Operativa	2	3	**Alto (6)**
Capacitación	2	2	**Medio (4)**
Infraestructura Tecnológica	3	3	**Crítico (9)**
Auditoría y Trazabilidad	3	3	**Crítico (9)**

Nota. La probabilidad se estimó según la frecuencia y severidad de vulnerabilidades detectadas mediante Wazuh, mientras que el impacto se evaluó en función de la afectación a la confidencialidad, integridad, disponibilidad y continuidad de los servicios institucionales.

La asignación de niveles de probabilidad se realizó en función de la intensidad de las vulnerabilidades y de su frecuencia real en función de los hallazgos de Wazuh. De este modo, se valoró probabilidad alta (3) cuando la evidencia indica una alta frecuencia para las vulnerabilidades de alta o intensidad crítica. Por ejemplo, la Infraestructura Tecnológica acumuló 1.659 vulnerabilidades de alta (49,49 %) y 3 de intensidad crítica, siendo el 76,19% de las vulnerabilidades publicadas correspondientes a 2025, lo cual justifica una probabilidad alta de que se materialice un incidente. También la Gestión de Incidentes y Auditoría recibió probabilidad alta

debido a que la alta frecuencia de hallazgos (3.352 vulnerabilidades) sumada al hecho de no haber procedimientos documentados y pistas de auditoría incrementa considerablemente la probabilidad de que pueda producirse un incidente sin ser gestionado. Los demás dominios recibieron probabilidad media (2) porque sí hay vulnerabilidades en ellos, pero la frecuencia de hallazgos de intensidad crítica o alta intensidad no era mayoritaria.

En consecuencia, las brechas identificadas representan no solo un problema técnico, sino también un riesgo legal y reputacional que justifica la implementación del plan propuesto.

Tabla 16. Análisis de brechas de ciberseguridad identificadas

Dominio	Brecha Identificada	Evidencia Wazuh	Métrica	Nivel de Riesgo	Referencia ISO/NIST
Gobernanza	Ausencia de políticas formales actualizadas y mecanismos de difusión sistemática.	Persistencia de vulnerabilidades como CVE-2025-15467 (OpenSSL) y CVE-2025-58098 (Apache) sin evidencia de gestión forma	3.352 hallazgos	Alto	ISO 27001 – A.5; NIST CSF – ID.GV
Control de Acceso	Revisión no periódica de permisos; ausencia de separación formal de roles y privilegios.	CVE en Apache como CVE-2025-66200 y CVE-2025-65082 permiten bypass de configuración y manipulación de variables	CVE Apache (High/ Medium)	Alto	ISO 27001 – A.5.15, A.5.18; NIST CSF – PR.AC
Gestión de Incidentes	Inexistencia de procedimientos documentados para el reporte y gestión de incidentes.	Vulnerabilidades críticas como CVE-2025-15467 y CVE-2025-69419 (OpenSSL) sin evidencia de tratamiento	1 Critical; 1.659 High	Crítico	ISO 27001 – A.5.26, A.5.27; NIST CSF – RS.RP

Continuidad Operativa	Planes de continuidad parcialmente implementados; sin pruebas formales documentadas.	CVE de disponibilidad en OpenSSL como CVE-2025-15467, CVE-2025-66199 (DoS) afectan continuidad del servicio	CVE OpenSSL (DoS)	Alto	ISO 27001 – A.5.29, A.5.30; NIST CSF – RC.RP
Capacitación	Capacitaciones no sistemáticas; brecha en conocimiento de procedimientos de respuesta.	Presencia de CVE en múltiples componentes (OpenSSL, Apache, urllib3 como CVE-2026-21441) evidencia falta de gestión técnica continua	Múltiples CVE High	Medio	ISO 27001 – A.6.3; NIST CSF – PR.AT
Infraestructura Tecnológica	Uso de PHP sin soporte técnico activo; bases de datos sin configuraciones robustas de seguridad.	Alta exposición en OpenSSL, Apache, kernel con CVE críticos y altos como CVE-2025-15467, CVE-2025-58098, CVE-2026-21441	3.352; 49% High	Crítico	ISO 27001 – A.8.8; NIST CSF – PR.IP, DE.CM
Auditoría y Trazabilidad	Inexistencia de pistas de auditoría que garanticen la trazabilidad de operaciones críticas.	CVE detectados (ej. CVE-2025-15467, CVE-2025-58098) sin evidencia de correlación ni auditoría de eventos	Sin trazabilidad completa	Crítico	ISO 27001 – A.8.15, A.8.17; NIST CSF – DE.AE

Nota. Nivel de riesgo determinado en función de la probabilidad de ocurrencia e impacto institucional.

Las brechas de mayor criticidad identificadas son la gestión informal de incidentes de seguridad, el uso de componentes tecnológicos obsoletos y la inexistencia de pistas de auditoría.

Estos hallazgos son consistentes con las vulnerabilidades descritas en el diagnóstico inicial de la institución y con las observaciones del experto entrevistado, confirmando la urgencia de intervención en dichos dominios. Adicionalmente, el análisis técnico del servidor web mediante herramientas de monitoreo permitió identificar vulnerabilidades con severidad alta, lo que evidencia una elevada exposición del sistema a amenazas potenciales. Del mismo modo, la existencia de carencias en componentes esenciales del entorno tecnológico indica también inadecuaciones en los procesos de actualización, configuración y endurecimiento de los sistemas; de forma análoga, el no contar con mecanismos formales de clasificación, de actualización y de respuesta a los eventos de seguridad determina la ineficiencia en la capacidad institucional de gestionar incidentes y de asegurar la trazabilidad de las operaciones, lo que refuerza la criticidad de las brechas detectadas.

3.7 PLAN DE FORTALECIMIENTO DE LA CIBERSEGURIDAD

Con los hallazgos del diagnóstico, y analizando las brechas identificadas, un Plan de Fortalecimiento de la Ciberseguridad se concibe para optimizar la salvaguarda de los sistemas tributarios del GAD municipal del cantón Salcedo. Este plan está calibrado con los controles ISO/IEC 27001:2022, el Marco de Ciberseguridad del NIST, y también la Ley Orgánica de Protección de Datos Personales (LOPDP). El detalle total de este plan, si desea verlo, aparece en el Anexo H.

Objetivo del plan.

Determinar acciones, controles y directrices técnicas y organizativas a fin de realzar la ciberseguridad en los sistemas tributarios del GAD municipal del cantón Salcedo. Ello, para acotar las brechas detectadas, preparando las prácticas institucionales según estándares internacionales y

la normativa nacional actual. Este plan se divide en tres horizontes, cada uno con su plazo definido. El corto plazo, de 0 a 4 meses, se enfoca en la contención y estabilización. Luego, el mediano plazo, abarcando 4 a 8 meses, será para la ejecución de la migración tecnológica. Finalmente, el largo plazo, de 8 a 12 meses, apuntará a lograr la optimización y madurez en ciberseguridad.

Alcance de la propuesta.

Es importante señalar que la presente investigación se limita al diseño y formulación del Plan de Fortalecimiento de la Ciberseguridad. No se ha implementado ninguna de las acciones aquí descritas, ni se ha evaluado su efectividad en el entorno real del GAD. La ejecución, el seguimiento y la validación del plan corresponden a una etapa posterior, que deberá ser asumida por las autoridades institucionales con sus propios recursos humanos, técnicos y financieros. Consecuentemente, no es la intención que los hallazgos de esta investigación se vean cual medición directa del efecto del plan, sino más bien una sugerencia detallada y justificada técnicamente. Para que le permita al GAD evaluar su aceptación y decidir la manera en que se implementará.

Componentes estratégicos.

La organización del plan se divide en cuatro pilares estratégicos, cada uno de los cuales responde a las deficiencias detectadas durante la fase de diagnóstico:

Componente 1: Gobernanza y Políticas de Seguridad.

Se incluyen aspectos como la creación y aprobación de una política de protección institucional, la constitución de un Comité de Seguridad Informática, y la elaboración de un inventario detallado de los bienes.

Componente 2: Control de Acceso y Protección de la Información.

Aborda aspectos como la definición de perfiles y roles, la implementación de autenticación de dos pasos (MFA), el cifrado de información sensible y la implementación de una política de uso de contraseñas seguras.

Componente 3 : Gestión de Incidentes, Continuidad de las Operaciones/Recuperación ante desastres y Auditoría.

Incluye aspectos como el diseño de un Procedimiento formal de Gestión de Incidentes , la implementación de registro en pistas de auditorías , la formalización de los respaldos y el diseño de un Plan de continuidad de las operaciones y recuperación ante desastres (BCP/DRP).

Componente 4: Actualización Tecnológica, Capacitación y Cultura de Ciberseguridad.

Se aborda la migración de sistemas a versiones de software reciente y que cuenten con soporte activo, el debido control de bases de datos, capacitación semestral en ciberseguridad, y procesos para la gestión de vulnerabilidades.

Horizontes de implementación.

Se organizan las acciones en tres horizontes, que contempla el desarrollo progresivo y priorizado:

Tabla 17. Diagrama de Gantt resumido por horizontes de implementación

Horizonte de implementación	Propósito general	0-4 meses	4-8 meses	8-12 meses
Corto plazo	Reducir riesgos críticos y estabilizar la base tecnológica y organizativa	[redacted]		

Horizonte de implementación	Propósito general	0-4 meses	4-8 meses	8-12 meses
Mediano plazo	Implementar controles técnicos y completar la remediación estructural		[redacted]	
Largo plazo	Consolidar la resiliencia y madurez en ciberseguridad			[redacted]

Nota. El diagrama presenta la distribución resumida de los horizontes de implementación del Plan de Fortalecimiento de Ciberseguridad en un período estimado de doce meses.

Tabla 18. Principales acciones

Horizonte	Acciones estratégicas
Corto plazo: 0-4 meses	Desarrollar políticas de seguridad, establecer un comité de seguridad, realizar inventarios de activos, perfiles y roles claros, política de gestión de contraseñas, procedimientos para manejar incidentes, proceso de respaldo, y comenzar con PHP.
Mediano plazo: 4-8 meses	Continuar con la migración a PHP, fortalecimiento de bases de datos, ejecución de auditorías, implementación de un sistema de autenticación multifactor (MFA), promoción de la concienciación institucional y gestión activa de vulnerabilidades.
Largo plazo: 8-12 meses	Construir el plan de continuidad del negocio y recuperación ante desastres (BCP/DRP), capacitación continua del personal, simulacros periódicos y evaluación sistemática para hacer un seguimiento de cuáles son los problemas, cómo solucionarlos y cómo manejarlos internamente.

Nota. Los plazos presentados son estimaciones y pueden ser ajustados según la capacidad técnica y las circunstancias operativas del GAD Municipal del cantón Salcedo.

El cronograma específico que detalla las acciones mensuales y las agrupaciones estratégicas se encuentra en la Tabla H.6 del Anexo H, sirviendo como complemento operativo para el diagrama de Gantt. Estos cronogramas son meramente referenciales y pueden ser alterados en función de los recursos técnicos disponibles y las condiciones operativas del GAD.

CONCLUSIONES

- El análisis determinó que el nivel de cumplimiento de la ciberseguridad es medio en comparación con estándares internacionales. La brecha más importante es la forma en que se manejan los incidentes de seguridad, ya que no hay procedimientos documentados y el servidor que aloja los sistemas tributarios es muy vulnerable. Esta brecha es muy grave y afecta directamente la confidencialidad, la integridad y la disponibilidad de la información, dando respuesta al objetivo general de la investigación.
- El análisis a partir de la herramienta Wazuh y la revisión de las capturas de los sistemas hicieron eco de manera objetiva las debilidades identificadas: la existencia de vulnerabilidades en sistemas tecnológicos, de prácticas de desarrollo inseguras y de la ausencia de controles de acceso y de auditoría. Ello confiere validez y consistencia a los resultados de la encuesta.
- La comparación entre la situación actual y la ISO/IEC 27001:2022, así como al NIST Cybersecurity Framework evidencia un bajo nivel de cumplimiento en dominios críticos de gobernanza, control de acceso, auditoría y gestión de vulnerabilidades, cuya existencia representa dificultades críticas que deben ser abordadas de inmediato.
- La matriz de riesgos construida a partir de la probabilidad y el impacto de las brechas, categorizó estas últimas en niveles bajo, medio, alto y crítico. La mayor parte de los dominios estudiados se localizan en los niveles alto y crítico, lo que indica que los sistemas tributarios están sometidos a amenazas internas y externas en alto grado y, por lo tanto, que se debe dar respuesta urgentemente con medidas estructurales.

- La combinación de encuestas (cuantitativo) con la evidencia técnica (cualitativo) promovió un análisis del problema. Las conclusiones no dependen solamente de lo dicho por la gente, sino también de lo visible para los sistemas, con lo que se asegura validez y confiabilidad.
- Los sistemas tributarios son activos críticos para el GAD Municipal del cantón Salcedo, ya que soportan procesos financieros y administrativos sensibles. Un incidente de seguridad podría implicar impactos técnicos, impactos legales e impactos sociales muy graves; por ello, es una prioridad actuar sobre la ciberseguridad.
- El Plan de Fortalecimiento de la Ciberseguridad propuesto responde de forma estructurada a las brechas identificadas y lo hace priorizando los dominios críticos, como: infraestructura tecnológica, gestión de incidentes y auditoría. Alineado con las mejores prácticas internacionales y con la normativa nacional; no obstante, el conseguir estos resultados va a depender de su implementación, seguimiento y evaluación en el entorno institucional.

RECOMENDACIONES

- Se recomienda a las autoridades del GAD municipal del cantón Salcedo designar un CISO o equivalente, cuya responsabilidad esté en el campo de la ciberseguridad. En este momento el jefe de TIC, hace frente a su carga administrativa y estratégica, lo que produce un menor esfuerzo en la protección de los activos de información.
- Establecer y formalizar políticas de seguridad de la información en consonancia con los estándares internacionales y con la normativa nacional vigente, para definir lineamientos claros de uso de los sistemas, de protección de los datos y de adjudicación de responsabilidades.
- Instaurar mecanismos formales de control de accesos basados en roles, en atención al principio de mínimo privilegio, con el fin de controlar las acciones de los usuarios a las funciones que les son propias y reducir el riesgo de acceso fraudulento.
- Establecer mecanismos de auditoría y trazabilidad, para verificar el registro de actividades en los sistemas tributarios que permitan garantizar la trazabilidad de las operaciones, el control interno y la determinación de incidentes.
- Aplicar un proceso gradual de actualización de los componentes tecnológicos (plataformas de desarrollo, bases de datos y servidores) con la finalidad de reducir la exposición a las vulnerabilidades de las tecnologías que se encuentran en desuso.
- Aplicar esquemas en ciberseguridad dirigidos al equipo institucional especialmente a la unidad de TIC, con miras a realzar su entrenamiento en el manejo de amenazas, la salvaguardia de los datos y la acción frente a eventos. Establecer lineamientos formales acerca de la administración de percances y la resiliencia, para la permanencia de las

operaciones y la recomposición post-contingencia, asegurando la operatividad de los sistemas de pago en coyunturas difíciles.

- Realizar procesos de seguimiento y evaluación, mediante indicadores de desempeño y auditorías internas, una vez implementadas las acciones derivadas de la presente investigación. Cabe indicar que la presente investigación se limita al análisis y propuesta de mejoras en materia de ciberseguridad, pero no contempla la implementación y evaluación del Plan, lo cual será una etapa posterior a desarrollar a nivel institucional.

REFERENCIAS

Andrade Alban, P. E. (2022). *La transformación digital en la mejora de los procesos de tributación*. https://repositorio.uisrael.edu.ec/handle/47000/2937

Asamblea Nacional del Ecuador. (2021). *Ley Orgánica de Protección de Datos Personales*. Registro Oficial Suplemento 459. https://www.telecomunicaciones.gob.ec/wp-content/uploads/2021/06/Ley-Organica-de-Datos-Personales.pdf

Banco Mundial. (2024). *Economía Digital para América Latina y el Caribe Diagnóstico de país: Ecuador.* Washington, D.C.: World Bank Publication. https://documents1.worldbank.org/curated/en/099028101262416449/pdf/IDU1814d30001e2a814b741bbf711771cfdc3a0b.pdf

Boné Andrade, M. F. (2023). *Evaluación de la evolución de la ciberseguridad en sistemas empresariales modernos*. Multidisciplinary Collaborative Journal, 1(2), 25-38. https://doi.org/10.70881/mcj/v1/n2/14

Cabezas Zambrano, L. S. (2025). *Transformación digital y su incidencia en la recaudación de tributos municipales en el Gobierno Autónomo Descentralizado del cantón Jipijapa*. http://repositorio.unesum.edu.ec/handle/53000/8137

Calle Córdova, M. J. (2025). *Impacto de la Digitalización en la Recaudación Tributaria: Desafíos y Oportunidades en el Sistema Fiscal Ecuatoriano.* Ciencia Latina Revista Científica Multidisciplinar, 9(2), 2832-2846. https://doi.org/10.37811/cl_rcm.v9i2.17098

Check Point Research. (2025). *Informe sobre el estado de la ciberseguridad, 2025*. Check Point Software Technologies Ltd. https://engage.checkpoint.com/resources-spanish/items/report-the-state-of-cyber-security-2025-es?fw=9484a

Elizalde Salazar, J. P. (2025). *Transformación digital en la administración de herramientas tributarias del Gobierno Autónomo Descentralizado Parroquial Membrillal 2023*. http://repositorio.unesum.edu.ec/handle/53000/8122

Hernández Sampieri, R., & Mendoza Torres, C. P. (2018). *Metodología de la investigación: Las rutas cuantitativa, cualitativa y mixta (1.ª ed.)*. McGraw-Hill Educación. https://bibliotecadigital.uce.edu.ec/s/L-D/item/793

International Organization for Standardization. (2018). *ISO/IEC 27005:2018 Information security risk management.* ISO. https://www.iso.org/obp/ui/#iso:std:iso-iec:27005:ed-3:v1:en

International Organization for Standardization. (2022). *ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection — Information security management systems — Requirements*. ISO. https://www.exactls.com/wp-content/uploads/2025/02/ISO_IEC-270012022-ed.3.pdf

Morán Chilán, J. H., & Pangay Sánchez, J. A. (2025). *Retos y desafíos del E-Gobierno en la administración tributaria.* Revista Científica Multidisciplinaria Arbitrada Yachasun - ISSN: 2697-3456, 9(17), 516-529. https://doi.org/10.46296/yc.v9i17.0708

Murillo Prado, K. P. (2022). *Analizar la metodología de gestión de vulnerabilidades para mejorar la seguridad en los sistemas informáticos en una institución financiera nacional*. https://repositorio.ucenfotec.ac.cr/handle/123456789/xmlui/handle/123456789/394

National Institute of Standards and Technology. (2024). *Framework for improving critical infrastructure cybersecurity (Version 2.0)*. NIST. https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf

Pico González, J. L., Quimis Pionce, J. M., Bacusoy Sánchez, C. L. & Choez Lino, M. N. (2024). *Impacto de las tecnologías en la administración presupuestaría y tributaria en el Ecuador*. Conocimiento global, 9(1), 252-259. https://doi.org/10.70165/cglobal.v9i1.359

PT Cyber Analytics. (2025). *Cybersecurity Threatscape for Latin America and the Caribbean: 2023–2024*. Group-IB, Positive Technologies. https://global.ptsecurity.com/en/research/analytics/cybersecurity-threatscape-for-latin-america-and-the-caribbean-2023-2024/?utm_source=chatgpt.com#Navigation-1

ANEXOS

Anexo A: Encuesta

Objetivo:

Recolectar información cuantitativa sobre la aplicación de políticas, controles y prácticas de ciberseguridad en los sistemas tributarios municipales, desde la percepción del personal técnico involucrado en su gestión.

Población objetivo:

Esta encuesta esta dirigida a los empleados de la Jefatura de Tecnologías de la Información y Comunicación (TIC) del GAD Municipal del Cantón Salcedo.

Instrumento:

Cuestionario en línea o impreso, distribuido en cuatro secciones.

Instrucciones para el participante:

Estimado(a) participante,

El objetivo de esta encuesta es evaluar el grado de implementación y adherencia a las políticas, controles y prácticas de ciberseguridad que se han establecido en los sistemas tributarios municipales.

Por favor, lea atentamente cada afirmación y marque con una (X) la opción que mejor refleje su nivel de acuerdo o desacuerdo, en base a la siguiente escala de valoración:

1 = Totalmente en desacuerdo

2 = En desacuerdo

3 = Ni de acuerdo ni en desacuerdo

4 = De acuerdo

5 = Totalmente de acuerdo

Sección 1. Gobernanza y políticas de seguridad

Ítem	Enunciado	Escala (1–5)
1	En la institución existen políticas formales de seguridad de la información aprobadas y vigentes.	1 ☐ 2 ☐ 3 ☐ 4 ☐ 5 ☐
2	Las políticas de seguridad son conocidas y difundidas entre los funcionarios que gestionan los sistemas tributarios.	1 ☐ 2 ☐ 3 ☐ 4 ☐ 5 ☐
3	Se realizan revisiones periódicas de cumplimiento de las políticas y procedimientos de seguridad.	1 ☐ 2 ☐ 3 ☐ 4 ☐ 5 ☐

Sección 2. Control de acceso y protección de la información

Ítem	Enunciado	Escala (1–5)
4	Los accesos a los sistemas tributarios se gestionan mediante credenciales personales asignadas a cada usuario.	1 ☐ 2 ☐ 3 ☐ 4 ☐ 5 ☐
5	Los permisos de acceso se asignan según las funciones de cada usuario y se revisan periódicamente.	1 ☐ 2 ☐ 3 ☐ 4 ☐ 5 ☐
6	La información sensible de los contribuyentes se gestiona bajo principios de confidencialidad e integridad.	1 ☐ 2 ☐ 3 ☐ 4 ☐ 5 ☐

Sección 3. Gestión de incidentes y continuidad operativa

Ítem	Enunciado	Escala (1–5)
7	Existen procedimientos documentados para reportar y gestionar incidentes de seguridad informática.	1 ☐ 2 ☐ 3 ☐ 4 ☐ 5 ☐
8	Los respaldos se almacenan en medios seguros y se realizan pruebas periódicas de recuperación.	1 ☐ 2 ☐ 3 ☐ 4 ☐ 5 ☐
9	La institución cuenta con mecanismos o planes de continuidad ante fallas o ataques informáticos.	1 ☐ 2 ☐ 3 ☐ 4 ☐ 5 ☐

Sección 4. Capacitación y cultura de ciberseguridad

Ítem	Enunciado	Escala (1–5)
10	El personal técnico recibe capacitaciones periódicas sobre buenas prácticas de ciberseguridad.	1 ☐ 2 ☐ 3 ☐ 4 ☐ 5 ☐
11	Se promueve la concienciación del personal respecto a la protección de la información institucional.	1 ☐ 2 ☐ 3 ☐ 4 ☐ 5 ☐
12	El personal conoce los pasos a seguir en caso de detectar una amenaza o vulnerabilidad en el sistema.	1 ☐ 2 ☐ 3 ☐ 4 ☐ 5 ☐

Sección de datos generales.

Por favor, complete los siguientes datos para fines de análisis:

- Cargo o función principal en el área TIC: _____

Tiempo de servicio en la institución:
☐ Menos de 2 años ☐ De 2 a 5 años ☐ Más de 5 años

- Nivel de formación académica:
  ☐ Tecnólogo ☐ Ingeniero ☐ Especialista o máster ☐ Otro: _____

Anexo B: Entrevista

ENTREVISTA TÉCNICA A UN EXPERTO

Título del proyecto: Plan de fortalecimiento de la ciberseguridad para los sistemas tributarios del GAD municipal del cantón Salcedo

Objetivo de la entrevista: Validar y enriquecer los hallazgos cuantitativos del cuestionario aplicado al personal TIC, desde una perspectiva técnica especializada en ciberseguridad, estándares internacionales y gestión de riesgos en el sector público.

Entrevistado: Profesional con experiencia en implementación de estándares internacionales de seguridad de la información y gestión de riesgos en el sector público.

Datos generales del entrevistado

Nombre del experto: _____

Cargo o función actual: _____

Preguntas de la entrevista

1. **Gobernanza y SGSI**

Desde su experiencia en el sector público municipal ecuatoriano, ¿cuál considera usted que es la principal brecha o debilidad en materia de ciberseguridad? ¿Qué papel juega la ausencia de un Sistema de Gestión de Seguridad de la Información (SGSI) formalmente estructurado?

2. **Control de acceso**

En entornos municipales donde los sistemas han sido desarrollados con tecnologías consideradas obsoletas, como versiones antiguas de PHP sin soporte activo, ¿cómo evalúa usted

la implementación de los controles de acceso? ¿Qué debilidades específicas observa en la gestión de privilegios y en la revisión periódica de permisos?

3. **Principio de mínimo privilegio**

En su opinión, ¿con qué frecuencia se aplica el principio de mínimo privilegio en las organizaciones públicas de baja madurez en ciberseguridad? ¿Qué consecuencias tiene su omisión?

4. **Gestión de incidentes**

¿Qué tan crítico considera usted que es, para un gobierno local, contar con procedimientos formalizados para la detección, clasificación y respuesta ante incidentes de seguridad? ¿Qué riesgos específicos implica la inexistencia de estos procesos?

5. **Capacitación y concienciación**

¿A qué grupos de funcionarios deberían dirigirse los programas de capacitación en ciberseguridad dentro de un GAD? ¿Con qué periodicidad recomendaría implementarlos y qué temas específicos deberían priorizarse?

Anexo C: Resultado de la encuesta

Tabla C.1 - Resultados de la encuesta

Marca temporal	1. En la institución existen políticas formales de seguridad de la información aprobadas y vigentes.	2. Las políticas de seguridad son conocidas y difundidas entre los funcionarios que gestionan los sistemas tributarios.	3. Se realizan revisiones periódicas de cumplimiento de las políticas y procedimientos de seguridad	4. Los accesos a los sistemas tributarios se gestionan mediante credenciales personales asignadas a cada usuario.	5. Los permisos de acceso se asignan según las funciones de cada usuario y se revisan periódicamente.	6. La información sensible de los contribuyentes se gestiona bajo principios de confidencialidad e integridad.	7. Existen procedimientos documentados para reportar y gestionar incidentes de seguridad informática.
2/3/2026 7:40	2	3	3	4	3	4	3
2/3/2026 23:09	2	3	3	4	3	4	3
4/3/2026 8:16	4	4	3	4	4	4	3
4/3/2026 11:35	3	3	3	4	4	3	3
5/3/2026 14:06	3	2	4	3	3	4	3
5/3/2026 16:07	4	3	3	3	4	4	3
5/3/2026 20:08	3	3	4	3	4	4	2

8. Los respaldos se almacenan en medios seguros y se realizan pruebas periódicas de recuperación.	9. La institución cuenta con mecanismos o planes de continuidad ante fallas o ataques informáticos.	10. El personal técnico recibe capacitaciones periódicas sobre buenas prácticas de ciberseguridad.	11. Se promueve la concienciación del personal respecto a la protección de la información institucional.	12. El personal conoce los pasos a seguir en caso de detectar una amenaza o vulnerabilidad en el sistema	Cargo o función principal en el área De TIC:	Tiempo de servicio en la institución:	Nivel de formación académica:
5	4	4	3	3	Analista	Menos de 2 años	Ingeniería
4	3	3	4	3	Analista	Más de 5 años	Ingeniería
5	4	3	5	5	Analista de Desarrollo	De 2 a 5 años	Ingeniería
4	3	3	3	2	Técnico de soporte	De 2 a 5 años	Ingeniería
4	3	3	3	3	Técnico de Soporte	De 2 a 5 años	Ingeniería
4	3	3	3	2	Analista	De 2 a 5 años	Ingeniería
4	3	3	3	3	Jefe	De 2 a 5 años	Ingeniería

Nota: Se describe resultados obtenidos.

Anexo D. Cálculo Alfa de Cronbach

Figura D.1 - Datos de la encuesta para cálculo de alfa de Cronbach

Sujeto	Item 1	Item 2	Item 3	Item 4	Item 5	Item 6	Item 7	Item 8	Item 9	Item 10	Item 11	Item 12	Total
1	2	3	3	4	3	4	3	5	4	4	3	3	41
2	2	3	3	4	3	4	3	4	3	3	4	3	39
3	4	4	3	4	4	4	3	5	4	3	5	5	48
4	3	3	3	4	4	3	3	4	3	3	3	2	38
5	3	2	4	3	3	4	3	4	3	3	3	3	38
6	4	3	3	3	4	4	3	4	3	3	3	2	39
7	3	3	4	3	4	4	2	4	3	3	3	3	39
8													
9													
10													
Varianzas	0,571	0,286	0,204	0,245	0,245	0,122	0,122	0,204	0,204	0,122	0,531	0,857	10,776

k=	12
V_i=	3,714
V_t=	10,776
α=	**0,715**

α : Alfa de Cronbach
k : Número de ítems
V_i: Varianza de cada ítem
V_t: Varianza del total

Nota: Resultados obtenidos para cálculo de alfa de cronbach

Confiabilidad del instrumento

Con el objetivo de evaluar la consistencia interna del instrumento aplicado, se calculó el coeficiente Alfa de Cronbach, donde se obtuvo un valor global de $\alpha = 0.715$, lo cual indica que el valor tiene un nivel aceptable de confiabilidad para el instrumento. Además, se analizó el Alfa de Cronbach si se elimina un elemento, esto se hizo para ver cómo contribuye cada ítem al comportamiento general del instrumento, los resultados muestran que eliminar la mayoría de los ítems no aumenta significativamente el valor global del alfa, lo cual confirma que el cuestionario es estable en general.

Para ser más transparentes en el análisis de confiabilidad, también se incluyó la correlación ítem-total, que mide como se relaciona cada ítem con el puntaje total del instrumento, sin incluir el ítem en el cálculo. Los ítems se correlacionan bien con el total corregido, esto significa que contribuyen adecuadamente a la consistencia interna. Los ítems 3 y 10 presentan correlaciones negativas, situación que se presenta por el reducido número de items por dimensión (solo 3) y por el pequeño tamaño de la muestra (n=7), condiciones en las que los coeficientes de correlación son más sensibles a la variabilidad natural de las respuestas. A pesar de estos valores, se decidió mantener ambos ítems porque son conceptualmente relevantes: el ítem 3 evalúa las revisiones periódicas de políticas claves para la gobernanza, y el ítem 10 evalúa la capacitación periódica del personal. Eliminar esos elementos habría resultado en que ambas dimensiones contaran únicamente con 2 ítems, lo que representa un problema estadístico aún mayor.

En resumen, aunque se identificaron elementos con una menor correlación estadística en relación al puntaje total, esto no afecta la confiabilidad general del instrumento. La desición de conservar estos elementos se fundamenta en criterios de relevancia teórica y su importancia dentro de las dimensiones evaluadas. Por lo tanto, el instrumento es considerado como confiable para el análisis propuesto.

Tabla D.1 – Análisis de confiabilidad del instrumento

Ítem	Alfa si se elimina	Correlación ítem-total
Ítem 1	0.730	0.185
Ítem 2	0.640	0.746
Ítem 3	**0.778**	**-0.456**
Ítem 4	0.704	0.292

Ítem	Alfa si se elimina	Correlación ítem-total
Ítem 5	0.726	0.103
Ítem 6	0.714	0.182
Ítem 7	0.725	0.054
Ítem 8	0.650	0.756
Ítem 9	0.650	0.756
Ítem 10	0.731	-0.018
Ítem 11	0.618	0.759
Ítem 12	0.593	0.805

Nota.- Cálculo de alfa por cada ítem si se elimina, y la correlación ítem-total corregida fue calculada correlacionando cada ítem con el puntaje total del instrumento, excluyendo el ítem evaluado.

Anexo E. Respuesta de la entrevista

Tabla E.1 - Respuestas a la entrevista aplicada

Marca temporal	Datos generales del entrevistado. Nombre del experto:	Cargo o función actual:	1. **Gobernanza y SGSI** Desde su experiencia en el sector público municipal ecuatoriano, ¿cuál considera usted que es la principal brecha o debilidad en materia de ciberseguridad? ¿Qué papel juega la ausencia de un Sistema de Gestión de Seguridad de la Información (SGSI) formalmente estructurado?	2. **Control de acceso** En entornos municipales donde los sistemas han sido desarrollados con tecnologías consideradas obsoletas, como versiones antiguas de PHP sin soporte activo, ¿cómo evalúa usted la implementación de los controles de acceso? ¿Qué debilidades específicas observa en la gestión de privilegios y en la revisión periódica de permisos?
11/5/2026 10:32	Roberto Ilbay	Jefe de Tecnologías de la Información y Comunicación	La deficiencia más obvia es la falta de un Sistema de Gestión de Seguridad de la Información (SGSI) formal. Las instituciones públicas municipales a menudo están regidas por controles de seguridad que están aislados, por lo que no es posible tener una política institucional que sirva como un marco unificado para la seguridad. La ausencia de un Sistema de Gestión de Seguridad de la Información (SGSI) limita la capacidad organizativa para abordar sistemáticamente los riesgos, establecer responsabilidades claras y asegurar la mejora continua en la protección de la información.	Aunque se emplean credenciales individuales como un control básico, existen notables debilidades en la gestión del acceso, especialmente en lo que respecta a la administración de privilegios y a la falta de revisiones periódicas sobre los permisos otorgados. El uso de tecnologías obsoletas incrementa la exposición a vulnerabilidades, dificultando la implementación de controles de seguridad robustos.

3. **Principio de mínimo privilegio** En su opinión, ¿con qué frecuencia se aplica el principio de mínimo privilegio en las organizaciones públicas de baja madurez en ciberseguridad? ¿Qué consecuencias tiene su omisión?	4. **Gestión de incidentes** ¿Qué tan crítico considera usted que es, para un gobierno local, contar con procedimientos formalizados para la detección, clasificación y respuesta ante incidentes de seguridad? ¿Qué riesgos específicos implica la inexistencia de estos procesos?	5. **Capacitación y concienciación** ¿A qué grupos de funcionarios deberían dirigirse los programas de capacitación en ciberseguridad dentro de un GAD? ¿Con qué periodicidad recomendaría implementarlos y qué temas específicos deberían priorizarse?
En instituciones con un bajo nivel de madurez en ciberseguridad, el principio de privilegio mínimo suele pasar por alto, permitiendo que los usuarios accedan a funciones o información no permitida, o que no son parte de sus funciones. Con esta omisión se genera un mayor riesgo de acceso no autorizado y el uso indebido de datos, imposibilitando el poder establecer la responsabilidad en situaciones que van en contra de la seguridad.	Como componente clave de la ciberseguridad, tenemos la gestión de incidentes. Cuando ocurre un incidente y no hay un procedimiento establecido, a la organización le resulta difícil actuar de manera adecuada y rápida. Sin dichos procesos, el documentar eventos, realizar un análisis posterior e implementar medidas correctivas, limita la capacidad de actuación ante un incidente, aumentando su impacto.	La capacitación en ciberseguridad debe dirigirse a todo el personal institucional, no solo al área técnica, ya que los usuarios son un factor crítico en la seguridad de la información. Los programas de concienciación deben implementarse al menos semestralmente, enfocándose en el phishing, la ingeniería social, la gestión segura de contraseñas y el uso adecuado de los sistemas.

Anexo F. Reporte de vulnerabilidades detectadas por Wazuh

Tabla F.1 - Listado de vulnerabilidades identificadas en el servidor

Agente	Paquete	Versión	Descripción	Severidad	CVE ID
servidorweb191	openssl-libs	1:3.2.2-16.el10_0.4	OpenSSL: Denial of Service via type confusion in PKCS#7 signature verification	Medium	CVE-2026-22796
servidorweb191	openssl-libs	1:3.2.2-16.el10_0.4	OpenSSL: Remote code execution via oversized Initialization Vector in CMS parsing	Critical	CVE-2025-15467
servidorweb191	kernel	6.12.0-55.40.1.el10_0	Linux kernel: Out-of-bounds write in fbdev leads to privilege escalation	High	CVE-2025-40304
servidorweb191	kernel	6.12.0-55.40.1.el10_0	Linux kernel: Use-after-free in proc_readdir_de() leads to privilege escalation	High	CVE-2025-40271
...	...	...	...	...	...

Nota: Se presenta un extracto representativo. El listado completo se encuentra disponible en el archivo digital adjunto, denominado Dataset Analisis_Wazuh_Servidor Web.

Anexo G. Autorización para el uso de información institucional con fines académicos.

Figura G.12. Autorización para el uso de información institucional con fines académicos

SALCEDO
GAD MUNICIPAL
ALCALDÍA

Of. Nº AL-720-2025-GADMCS-A1.

San Miguel de Salcedo, 11 de noviembre del 2025.

Ing. Paulina Villalba
Analista de Tecnologías de la Información y Comunicación.
Presente.-

De mi consideración:

En atención a su solicitud mediante oficio N. TICS-001-2025, en la cual pone en conocimiento que se encuentra cursando la Maestría en Ciberseguridad en la Universidad Estatal Península de Santa Elena (UPSE), y considerando el desarrollo de su trabajo de titulación denominado: **"Plan de fortalecimiento de la ciberseguridad para los sistemas tributarios del GAD Municipal del cantón Salcedo, basado en estándares de seguridad"**, me permito manifestar lo siguiente:

Esta Autoridad **AUTORIZA** el uso de información institucional estrictamente necesaria para el desarrollo de su investigación académica, siempre y cuando dicho acceso, tratamiento y análisis de la información se realice bajo criterios de confidencialidad, responsabilidad y uso adecuado.

Se deja expresa constancia de que la información deberá ser utilizada exclusivamente con fines académicos, evitando su divulgación, reproducción o uso indebido, en cumplimiento de la normativa vigente, en especial lo dispuesto en la Ley Orgánica de Protección de Datos Personales (LOPDP), así como las políticas internas de seguridad de la información de la institución.

Adicionalmente, se dispone que los datos sensibles o críticos sean debidamente anonimizados o tratados de forma agregada, garantizando la protección de la información institucional y evitando cualquier riesgo que pudiera afectar la integridad, confidencialidad o disponibilidad de los activos de información.

Finalmente, se exhorta a que los resultados obtenidos en el marco de la investigación puedan ser compartidos con la institución, a fin de que estos contribuyan al fortalecimiento de la gestión de ciberseguridad y mejora continua de los sistemas institucionales.

Sin otro particular, reitero mi apoyo a las iniciativas académicas que aporten al desarrollo institucional.

Atentamente,

Ing. Juan Paúl Pacheco Velásquez.
ALCALDE DEL GAD MUNICIPAL
DEL CANTÓN SALCEDO

JPPV/jch

GAD MUNICIPAL DEL CANTÓN SALCEDO
Calle Bolívar y Sucre esquina, frente al Parque Central
Teléfono: 032700-420 Ext. 100
Correo electrónico: juanpaul.pacheco@salcedo.gob.ec
Teléfono: 0984106977

Nota: Imagen hace referencia a la autorización concedida por la Máxima Autoridad del GAD municipal del cantón Salcedo, para el uso de información institucional con fines académicos.

Anexo H. Plan de Fortalecimiento de la Ciberseguridad

PLAN DE FORTALECIMIENTO DE LA CIBERSEGURIDAD

El Plan de Fortalecimiento de la Ciberseguridad es una propuesta de diseño académico elaborada como parte de una investigación. El contenido del plan aborda aspectos importantes como: acciones, plazos, cronogramas, indicadores y presupuesto. Y ha sido desarrollado bajo análisis realizado al GAD Municipal del cantón Salcedo, de forma particular se verificó la infraestructura tecnológica actual, el uso de sistemas tributarios que han sido desarrollados internamente en el GAD, y el nivel de madurez en ciberseguridad. Este documento sirve como marco referencial y estimativo, y no como una directríz definitiva.

La ejecución efectiva del plan, que abarca la asignación de recursos humanos, tecnológicos y financieros, así como la validación de los costos y tiempos propuestos aquí deben ser evaluados, modificados y aprobados por las autoridades del GAD municipal del cantón Salcedo, conforme a sus procedimientos administrativos, disponibilidad presupuestaria y capacidades operativas.

Esta investigación se limita al diagnóstico y la propuesta; no incluye la ejecución ni la evaluación del plan en el entorno real de la institución. La metodología utilizada tiene la virtud de que los elementos detectados sean susceptibles de ser transferidos y adaptados a otros GAD que presentan las características similares que caracterizan a este GAD.

1. INTRODUCCION

A partir del diagnóstico elaborado de la situación actual, del análisis de brechas y de los lineamientos concretos establecidos conforme a la norma ISO/IEC 27001:2022, el NIST

Cybersecurity Framework y la Ley Orgánica de Protección de Datos Personales (LOPDP), se desarrolla a continuación el Plan de Fortalecimiento de la Ciberseguridad para los sistemas tributarios del GAD municipal del cantón Salcedo. El Plan se organiza en cuatro componentes estratégicos orientados hacia la mitigación de las vulnerabilidades identificadas y el aseguramiento de las dimensiones de confidencialidad, integridad y disponibilidad de la información tributaria institucional.

2. OBJETIVO DEL PLAN

Establecer un conjunto de acciones, controles y lineamientos técnicos y organizativos que permitan fortalecer la ciberseguridad en los sistemas tributarios del GAD municipal del cantón Salcedo, reduciendo las brechas identificadas y alineando las prácticas institucionales con los estándares internacionales de seguridad de la información y la normativa nacional vigente.

Para ello, el plan se estructura en tres horizontes de implementación, priorizando la mitigación de riesgos críticos de infraestructura tecnológica y la progresiva madurez en ciberseguridad:

- Corto plazo (0–4 meses): Contención y estabilización.
- Mediano plazo (4-8 meses): Ejecución de la migración.
- Largo plazo (8-12 meses): Optimización y madurez.

3. ALCANCE Y VIGENCIA

La presente propuesta es un plan de ciberseguridad con alcance exclusivo para el diseño y la formulación de los controles, acciones y lineamientos expuestos. No incluye la implementación, ejecución ni evaluación de los mismos en el entorno real del GAD. Corresponde a las autoridades

institucionales, en una fase posterior, decidir si adoptan el plan, asignar los recursos necesarios y ejecutarlo.

El plan tiene un horizonte de implementación estimado de doce (12) meses, pero su vigencia real dependerá de la decisión institucional. Esta investigación se limita, pues, a la entrega de una propuesta como instrumento de apoyo a la toma de decisiones.

4. ESTRUCTURA DEL PLAN DE FORTALECIMIENTO

El Plan de Fortalecimiento de la Ciberseguridad se organiza en cuatro componentes estratégicos, puesto que cada uno de ellos responde con exactitud a las brechas detectadas en el diagnóstico y se encuentra alineado, en cuanto a sus contenidos, con los dominios de la norma inglesa ISO/IEC 27001:2022, las funciones identificadas del Framework del NIST y los principios de la Ley de Protección de Datos Personales (LOPDP). Dichos componentes y su alcance responden a las dimensiones de la ciberseguridad institucional desde la base organizativa y normativa, pasando por los controles de acceso y la protección de la información, la capacidad de respuesta ante incidentes, la continuidad operativa, la integración de la tecnología de la información y comunicación y la cultura de la ciberseguridad.

A continuación, se desarrolla cada componente con sus respectivas acciones, responsables, plazos y referencias normativas.

4.1 COMPONENTE 1: GOBERNANZA Y POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

Tabla H. 1 - Acciones del Componente 1: Gobernanza y Políticas

N°.	Acción	Responsable	Plazo	Referencia Normativa
1.1	Elaborar y aprobar formalmente una Política de Seguridad de la Información institucional, alineada con ISO/IEC 27001:2022 y la LOPDP.	Jefe de TIC / Dirección Administrativa	0–3 meses	ISO 27001 – A.5.1; LOPDP Art. 10
1.2	Socializar y difundir la política de seguridad a todo el personal TIC mediante talleres presenciales documentados.	Jefe de TIC	3–4 meses	ISO 27001 – A.5.1; NIST CSF – ID.GV-1
1.3	Establecer un calendario de revisión anual de políticas y procedimientos de seguridad, con actas de reunión y registros de actualización.	Jefe de TIC / Comité de Seguridad	4–6 meses	ISO 27001 – A.5.1; NIST CSF – ID.GV-4
1.4	Conformar un Comité de Seguridad de la Información con definición de roles, responsabilidades y mecanismos de supervisión.	Dirección Administrativa / TIC	2–4 meses	ISO 27001 – A.5.2; NIST CSF – ID.GV-2
1.5	Desarrollar e implementar un inventario clasificado de activos de información de los sistemas tributarios.	Jefe de TIC / Analistas	1–3 meses	ISO 27001 – A.5.9, A.5.10; NIST CSF – ID.AM

Nota. Información con base en los resultados del diagnóstico y los estándares ISO/IEC 27001:2022 y NIST CSF (2026).

4.2 COMPONENTE 2: CONTROL DE ACCESO Y PROTECCIÓN DE LA INFORMACIÓN

Tabla H.2 - Acciones del Componente 2: Control de Acceso

N°.	Acción	Responsable	Plazo	Referencia Normativa
2.1	Definir y documentar formalmente los perfiles de usuario y roles de acceso en los sistemas tributarios, aplicando el principio de mínimo privilegio.	Jefe de TIC / Analistas	1–3 meses	ISO 27001 – A.5.15, A.5.18; NIST CSF – PR.AC-1
2.2	Implementar un proceso formal de revisión semestral de permisos de acceso, con documentación de altas, bajas y modificaciones.	Jefe de TIC	3–5 meses	ISO 27001 – A.5.18; NIST CSF – PR.AC-3
2.3	Implementar la autenticación multifactor (MFA) para los accesos a los sistemas tributarios y a la infraestructura de servidores.	Analistas / Jefe de TIC	4–6 meses	ISO 27001 – A.5.17; NIST CSF – PR.AC-7
2.4	Establecer controles de cifrado para la transmisión y almacenamiento de información sensible de los contribuyentes.	Analista de Desarrollo / TIC	6–10 meses	ISO 27001 – A.8.24; NIST CSF – PR.DS-2
2.5	Implementar una política de contraseñas seguras con requisitos mínimos de longitud, complejidad y renovación periódica.	Jefe de TIC / Analistas	1–2 meses	ISO 27001 – A.5.17; NIST CSF – PR.AC-1

Nota. Información con base en los resultados del diagnóstico y los estándares ISO/IEC 27001:2022 y NIST CSF (2026).

4.3 COMPONENTE 3: GESTIÓN DE INCIDENTES, CONTINUIDAD OPERATIVA Y AUDITORÍA

Tabla H.3 - Acciones del Componente 3: Incidentes, Continuidad y Auditoría

N°.	Acción	Responsable	Plazo	Referencia Normativa
3.1	Diseñar y aprobar un procedimiento formal de gestión de incidentes de seguridad: clasificación, notificación, respuesta y cierre.	Jefe de TIC / Comité de Seguridad	1–3 meses	ISO 27001 – A.5.26, A.5.27; NIST CSF – RS.RP
3.2	Implementar pistas de auditoría en los sistemas tributarios para registrar accesos, modificaciones y operaciones críticas.	Analista de Desarrollo / TIC	3–7 meses	ISO 27001 – A.8.15, A.8.17; NIST CSF – DE.AE
3.3	Formalizar y documentar los procesos de respaldo de información, con definición de frecuencias, medios de almacenamiento y procedimientos de restauración verificados.	Técnicos de Soporte / TIC	2–4 meses	ISO 27001 – A.8.13; NIST CSF – PR.IP-4
3.4	Elaborar e implementar un Plan de Continuidad del Negocio (BCP) y un Plan de Recuperación ante Desastres (DRP) para los sistemas tributarios.	Jefe de TIC / Dirección Administrativa	6–10 meses	ISO 27001 – A.5.29, A.5.30; NIST CSF – RC.RP
3.5	Planificar y ejecutar simulacros anuales de recuperación ante incidentes, con documentación de resultados y lecciones aprendidas.	Jefe de TIC / Todo el equipo TIC	10–12 meses	ISO 27001 – A.5.30; NIST CSF – RC.IM

Nota. Información con base en los resultados del diagnóstico y los estándares ISO/IEC 27001:2022 y NIST CSF (2026).

4.4 COMPONENTE 4: ACTUALIZACIÓN TECNOLÓGICA, CAPACITACIÓN Y CULTURA DE CIBERSEGURIDAD

Tabla H.4 - Acciones del Componente 4: Tecnología, Capacitación y Cultura

N°.	Acción	Responsable	Plazo	Referencia Normativa
4.1	Planificar la migración de los sistemas tributarios a versiones actualizadas y con soporte técnico activo del lenguaje de programación (sustitución de PHP obsoleto).	Analista de Desarrollo / Jefe TIC	6–12 meses	ISO 27001 – A.8.8; NIST CSF – PR.IP-12
4.2	Aplicar un endurecimiento (*hardening*) de la configuración de las bases de datos, incluyendo control de acceso, cifrado en reposo y desactivación de servicios innecesarios.	Analistas / Técnicos de Soporte	4–8 meses	ISO 27001 – A.8.9; NIST CSF – PR.IP-1
4.3	Implementar un programa de capacitación semestral en ciberseguridad para el personal TIC, con módulos sobre: gestión de contraseñas, phishing, respuesta a incidentes y normativa vigente.	Jefe de TIC / RRHH Institucional	3–6 meses	ISO 27001 – A.6.3; NIST CSF – PR.AT-1
4.4	Desarrollar materiales de concienciación sobre protección de	Jefe de TIC / Comité de Seguridad	4–6 meses	ISO 27001 – A.6.3; NIST CSF – PR.AT-2

	información institucional dirigidos a todos los funcionarios que interactúan con los sistemas tributarios.			
4.5	Establecer un proceso de gestión de vulnerabilidades técnicas con análisis periódico (trimestral), priorización de parches basado en la explotación activa conocida y registro de hallazgos.	Analistas / Jefe de TIC	5–9 meses	ISO 27001 – A.8.8; NIST CSF – ID.RA, DE.CM

Nota. Información con base en los resultados del diagnóstico y los estándares ISO/IEC 27001:2022 y NIST CSF (2026).

La migración desde la versión de PHP 5.4.16 a una versión moderna como PHP 7 o 8, no es una simple actualización automática, implica un proceso de cambio de código, porque algunas extensiones fundamentales como mysql_query fueron eliminadas por completo. En lugar de las funciones actuales, se deben sustituir manualmente por alternativas seguras como PDO (PHP Data Objects) o MySQLi. Para lo cual, el GAD debe examinar y modificar partes esenciales del código fuente de los sistemas tributarios. Se recomienda también que el GAD asigne personal con experiencia en este tipo de migración y que contemple una fase de pruebas para prevenir posibles problemas en el servicio. Un plazo de 6 a 12 meses se estima que es razonable siempre que haya desarrolladores especializados y disponibles, aunque este tiempo puede variar según la disponibilidad de dichos profesionales.

5. Horizontes de implementación

Después de establecer las acciones en cada componente estratégico, estas se organizan en tres horizontes de implementación para garantizar su desarrollo progresivo, priorizar las acciones

sobre los riesgos críticos y garantizar la continuidad del plan en el tiempo. La planificación se basa por lo tanto en un enfoque en capas: comienza estabilizando la infraestructura tecnológica y disminuyendo el riesgo inmediato, continúa implementando controles de seguridad y finalizando con la estabilización de la madurez en ciberseguridad. A continuación, se presenta la distribución de las acciones por horizonte:

Tabla H. 5 - Acciones por período de tiempo

Horizonte	Período	Propósito	Acciones clave
Corto plazo	0-4 meses	Reducir riesgos críticos y estabilizar la base tecnológica y organizativa	Análisis y diagnóstico de sistemas, inicio de migración tecnológica (PHP), mitigación de vulnerabilidades críticas, políticas de seguridad, controles básicos de acceso, procedimientos de incidentes
Mediano plazo	4-8 meses	Implementar controles técnicos y completar la remediación estructural	Ejecución de migración tecnológica, MFA, pistas de auditoría, *hardening* de bases de datos, capacitación técnica y concienciación
Largo plazo	8-12 meses	Consolidar la resiliencia y madurez en ciberseguridad	Cifrado de información, planes de continuidad (BCP/DRP), simulacros, gestión continua de vulnerabilidades y mejora continua

Nota: Información en base a los resultados de las acciones identificadas en los componentes

6. CRONOGRAMA GENERAL DE IMPLEMENTACIÓN

La Tabla H.6 presenta la distribución temporal de las acciones del plan en el horizonte de doce meses, permitiendo visualizar la secuencia y solapamiento de actividades en cada componente estratégico. Es importante señalar que los plazos aquí establecidos tienen un carácter estimativo y referencial, no vinculante. En particular, la migración de PHP depende de la disponibilidad de personal técnico y de la complejidad técnica del entorno, por lo tanto, se

recomienda que el GAD municipal del cantón Salcedo considere un plan de contingencia ante posibles retrasos, ajustando los tiempos según su realidad operativa y capacidades institucionales.

Tabla H.6 - Cronograma general del Plan de Fortalecimiento de Ciberseguridad

Acción	M1	M2	M3	M4	M5	M6	M7	M8	M9	M10	M11	M12
1.1 Política de Seguridad	X	X	X									
1.4 Comité de Seguridad		X	X	X								
1.5 Inventario de activos	X	X	X									
2.1 Perfiles y roles	X	X	X									
2.5 Política de contraseñas	X	X										
3.1 Procedimiento de incidentes	X	X	X									
3.3 Respaldos formalizados		X	X	X								
4.1 Migración PHP	X	X	X	X	X	X	X	X				
4.2 *Hardening* BD				X	X	X	X	X				
3.2 Pistas de auditoría				X	X	X	X	X				
2.3 MFA				X	X	X	X					
4.4 Concienciación				X	X	X	X					
4.5 Gestión de vulnerabilidades					X	X	X	X	X			
3.4 BCP/DRP						X	X	X	X	X		
4.3 Programa capacitación									X	X	X	X
3.5 Simulacros									X	X	X	X

Nota. M = Mes.

7. INDICADORES DE SEGUIMIENTO Y CONTROL

Para garantizar el cumplimiento y la efectividad del plan, se establecen los indicadores de seguimiento presentados en la Tabla H.7, los cuales permiten medir el avance de las acciones y el impacto de las mejoras implementadas.

Tabla H.7 - Indicadores de seguimiento del Plan de Fortalecimiento

Componente	Indicador	Meta	Medio de Verificación
Gobernanza	% de políticas de seguridad formalizadas y aprobadas	100% al mes 3	Documento aprobado con firma institucional
Gobernanza	% de activos de información inventariados	100% al mes 3	Inventario institucional documentado
Control de Acceso	% de usuarios con roles y perfiles definidos	100% al mes 3	Matriz de roles y accesos
Control de Acceso	% de cumplimiento de política de contraseñas	100% al mes 2	Configuración de políticas en sistemas
Gestión de Incidentes	% de implementación del procedimiento de incidentes	100% al mes 3	Documento aprobado y registros de uso
Respaldo de Información	% de procesos de respaldo formalizados	100% al mes 4	Procedimientos documentados y evidencias de ejecución
Tecnología (Migración)	% de avance en la migración tecnológica (PHP)	30% al mes 4; 70% al mes 8; 100% al mes 10	Reportes de avance técnico
Tecnología (*Hardening*)	% de bases de datos con *hardening* aplicado	100% al mes 8	Evidencia de configuración segura

Auditoría	% de sistemas con pistas de auditoría activas	100% al mes 8	Logs habilitados y reportes
Control de Acceso (MFA)	% de accesos críticos con MFA implementado	100% al mes 7	Evidencia de implementación MFA
Capacitación / Cultura	% de personal concienciado en seguridad	100% al mes 7	Registros de talleres y difusión
Gestión de Vulnerabilidades	% de vulnerabilidades gestionadas en ciclos definidos	80% al mes 9	Reportes de gestión de vulnerabilidades
Continuidad	% de implementación de BCP/DRP	100% al mes 10	Documento aprobado
Capacitación Técnica	% del personal TIC capacitado	100% al mes 12	Certificados / registros
Continuidad	Número de simulacros ejecutados	1 al mes 12	Acta de simulacro

Nota. Los indicadores deberán ser evaluados trimestralmente por el Comité de Seguridad de la Información.

Las metas establecidas con 100% representan escenarios ideales de ejecución, basados en la disponibilidad técnica del equipo. Sin embargo, en la práctica institucional de un GAD municipal, los tiempos administrativos pueden extender estos plazos. Por lo tanto, las fechas son referenciales y orientativas, se recomienda al Comité de Seguridad de la Información monitorear el avance real y ajustar los cronogramas según la capacidad operativa y los ritmos administrativos de la institución.

En el indicador que mide el porcentaje de componentes tecnológicos que se han actualizado a versiones compatibles como el lenguaje PHP, establecemos un objetivo constante del 100% en

12 meses. Este objetivo se complementará con un plan por fases como se describe en el cronograma del plan. La migración se llevará a cabo gradualmente durante los primeros 10 meses e incluirá análisis, refactorización, pruebas y despliegue, para que el equipo técnico pueda realizar su trabajo sin interrupciones.

8. SÍNTESIS DEL PLAN Y ALINEACIÓN CON ESTÁNDARES

El Plan de Fortalecimiento de la Ciberseguridad propuesto integra veinte acciones distribuidas en cuatro componentes estratégicos, orientadas a subsanar las brechas identificadas en el diagnóstico y a elevar el nivel de madurez en ciberseguridad del GAD Municipal del cantón Salcedo. La Tabla H.8 presenta la alineación del plan con las funciones del NIST Cybersecurity Framework y los dominios de la norma ISO/IEC 27001:2022.

Tabla H.8 - Alineación del plan con ISO/IEC 27001:2022 y NIST CSF

Componente del Plan	Función NIST CSF	Cláusulas ISO 27001:2022	Alineación LOPDP
Gobernanza y Políticas	Identificar (ID.GV)	A.5.1, A.5.2, A.5.9	Art. 10 – Principio de seguridad
Control de Acceso	Proteger (PR.AC)	A.5.15, A.5.18, A.5.17, A.8.24	Art. 10 – Confidencialidad e integridad
Gestión de Incidentes	Responder (RS.RP, RS.AN)	A.5.26, A.5.27, A.5.28	Art. 39 – Notificación de incidentes
Continuidad Operativa	Recuperar (RC.RP, RC.IM)	A.5.29, A.5.30, A.8.13	Art. 10 – Disponibilidad
Actualización Tecnológica	Proteger (PR.IP); Detectar (DE.CM)	A.8.8, A.8.9, A.8.15	Art. 10 – Medidas técnicas adecuadas
Capacitación y Cultura	Proteger (PR.AT)	A.6.3	Art. 10 – Gestión de riesgos

Nota. Componentes alineados con las cláusula ISO y LOPDP

En síntesis, el plan de fortalecimiento propuesto constituye una respuesta integral, sistemática y fundamentada en estándares internacionales a las brechas de ciberseguridad identificadas en los sistemas tributarios del GAD Municipal del cantón Salcedo. Su implementación, bajo el seguimiento del Comité de Seguridad de la Información y con el compromiso de las autoridades institucionales, permitirá elevar el nivel de madurez en ciberseguridad, reducir la exposición a incidentes y fortalecer la protección de la información de los contribuyentes, en cumplimiento de las exigencias normativas vigentes y de las mejores prácticas internacionales en la materia.

9. PRESUPUESTO ESTIMADO

La implementación del presente plan requiere la asignación de recursos humanos, tecnológicos y financieros. A continuación, se presenta una estimación de los recursos necesarios para cada componente, misma que deberá ser validada y ajustada por las autoridades institucionales previo a su ejecución.

Cabe señalar que el presupuesto estimado tiene un carácter referencial, y su financiamiento deberá ser gestionado por la Dirección Financiera del GAD, quién definirá las fuentes de recursos para su implementación durante los meses contemplados en el plan. Adicionalmente es necesario mencionar que los valores estimados no incluyen IVA, ni otros impuestos aplicables, tampoco consideran costos de mantenimiento anual, renovación de licencias posteriores al primer año, ni actualizaciones tecnológicas futuras.

Tabla H.9 - Estimación de presupuesto para aplicación del plan

Componente	Acciones asociadas	Rubros de gasto	Tipo de recurso	Costo estimado (USD)

1: Gobernanza y Políticas	1.1, 1.2, 1.3, 1.4, 1.5	Elaboración de políticas, talleres internos	Interno	$ 0.00
		Material de difusión y apoyo (impresos/digitales)	Externo	$ 700.00
Subtotal				**$ 700.00**
2: Control de Acceso	2.1, 2.2, 2.3, 2.4, 2.5	Implementación de MFA	Externo	$1.800
		Licencias de gestión de identidades	Externo	$1.500
		Configuración y gestión de accesos	Interno	$0.00
Subtotal				**$3.300**
3: Incidentes, Continuidad y Auditoría	3.1, 3.2, 3.3, 3.4, 3.5	Configuración de monitoreo y logs	Interno	$0.00
		Almacenamiento para respaldos	Externo	$1.500
		Consultoría BCP/DRP	Externo	$3.000
Subtotal				**$4.500**
4: Tecnología, Capacitación y Cultura	4.1, 4.2, 4.3, 4.4, 4.5	Actualización y refactorización de sistemas (migración progresiva)	Interno	$0.00
		Herramientas de apoyo técnico: Licencia anual de escáner de vulnerabilidades (OpenVas)/Licencia de software de pruebas de penetración (Burp Suite Professional).	Externo	$2.000

		Cursos de formación especializada.	Externo	$1.500
Subtotal				**$3.500**
Capacitación complementaria	Capacitación flexible frente a tecnologías emergentes o hallazgos de vulnerabilidades	Taller práctico para solución de incidentes para el equipo de TIC.	Externo	$1.000
Soporte técnico urgente	Fondo destinado a imprevistos no considerados en otras categorías	Renovación urgente de licencias expiradas, ajustes no anticipados en la migración de PHP, o necesidad de horas adicionales para consultoría especializada.	Externo	$2.000
TOTAL ESTIMADO				**$15.000**

Nota: Los costos citados en la tabla, son estimados pudiendo variar de acuerdo a las condiciones del mercado, la negociación con proveedores y la existencia de recursos internos. Se hace impresindible que la Jefatura TIC elabore un presupuesto pormenorizado, para que sea aprobado por la Dirección Financiera.

Aquellas actividades cuyo tipo de recurso están clasificadas como "Interno", tienen un costo de cero dólares ($ 0.00) porque son labores que estarían a cargo del personal de la Jefatura TIC, cuyos salarios son parte del presupuesto regular del GAD. Por ende, estas tareas no generan un gasto adicional en efectivo. Sin embargo, si tiene un costo para la institución, este es el costo de oportunidad, que significa que el tiempo que un funcionario destina a la ejecución del plan, dejará de atender sus funciones operativas habituales. Se recomienda planificar las cargas laborales para evitar desatender la operación diaria.

Sobre los recursos externos, los valores estimados para MFA, licencias, consultoría, herramientas técnicas y capacitación, se calcularon con base en referencias del mercado

tecnológico ecuatoriano a la fecha de este estudio (2026). Previo a la ejecución, la Jefatura TIC deberá solicitar cotizaciones vigentes a proveedores locales para validar y ajustar los montos según las condiciones actuales del mercado.

10. CONCLUSIONES

- El Plan de Fortalecimiento de la Ciberseguridad propone una forma general y bien estructurada de hacer frente a las principales brechas que se dieron en los sistemas tributarios del GAD municipal del cantón Salcedo, a incrementar las dimensiones organizativa, técnica y normativa mediante cuatro componentes estratégicos: Gobernanza, Control de Acceso, Gestión de Incidentes y Continuidad Operativa y Actualización Tecnológica y Capacitación; el plan, en este sentido, provoca la base para la reducción de las brechas existentes. También es necesario apuntar que las acciones que contiene el plan son claramente tendentes a la disminución de riesgos; en el mismo orden de ideas, el hecho de que sea posible mitigar las brechas existentes también está supeditado a su ejecución, seguimiento y evaluación en el contexto institucional.

- La organización del plan en tres horizontes de implementación (corto, mediano y largo plazo) permite una ejecución progresiva y priorizada, garantizando que las acciones más urgentes sean abordadas en los primeros meses.

- El plan está alineado a los estándares internacionales ISO/IEC 27001:2022 y NIST Cybersecurity Framework, así como a la normativa ecuatoriana conocida por sus siglas como LOPDP, con el propósito de garantizar que las acciones propuestas responden a

mejores prácticas y exigencias de las normativas vigentes relacionadas con la seguridad de la información.

- El plan de fortalecimiento contemplado en este documento, presenta es una propuesta de diseño, que no se ha implementado, ni evaluado. Por tanto, las conclusiones se refieren a la coherencia y relevancia técnica del plan en relación con las brechas identificadas, más no, a su efectividad en operación real.

11. RECOMENDACIONES

Para la Institución:

- Aprobar formalmente el Plan de Fortalecimiento de la Ciberseguridad mediante resolución administrativa que lo haga vinculante, asignando los recursos humanos, tecnológicos y económicos necesarios para su ejecución, según el presupuesto estimado.
- Configurar el Comité de Seguridad de la Información durante el plazo establecido (dos a cuatro meses), nombrando encargados por cada tarea y fijando la frecuencia de los encuentros para vigilar el progreso del plan.
- Llevar a cabo una comprobación técnica de las propuestas, tomando en cuenta a los medios disponibles, el potencial de funcionamiento del departamento TIC y la congruencia con los plazos del proyecto.
- Establecer directrices precisas para priorizar las tareas, fundamentándose en el grado de peligro, la importancia de los sistemas y la repercusión general, para que esto sirva de pilar para su posterior aceptación.

- Definir un esquema de evaluación que permita, en una fase posterior, medir el impacto del plan mediante indicadores cuantitativos y cualitativos, tomando como referencia el diagnóstico inicial.

Para futuros investigadores académicos

- Promover la adecuada documentación del plan y su estructura metodológica, de manera que pueda ser utilizado como guía para su adaptación en otras instituciones públicas con características similares.
- Incorporar en el documento lineamientos orientados a la mejora continua, que permitan su actualización periódica en función de cambios en el entorno tecnológico, normativo y de riesgos.
- Los estudios futuros propuestos no solo deben diseñar planes, sino también aplicar y evaluar los planes en su mundo real. Esto podría hacerse a través de un estudio piloto en una de las áreas de GAD o mediante un análisis cuasi-experimental comparando la situación actual con la anterior, para medir la efectividad del plan.
- Se sugiere que este enfoque sea adoptado en otros GAD municipales que tienen sus propios sistemas de desarrollo y tecnologías obsoletas, y realizar un diagnóstico comparativo; identificar patrones de vulnerabilidad, resaltar buenas prácticas y formular recomendaciones.