GRUPO BLR

TOMO I

GESTIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN: UNA PERSPECTIVA DEL CONTROL INTERNO EN EL SECTOR PÚBLICO

Byron Napoleón Cadena Oleas
Raquel Virginia Colcha Ortiz
Wilmer Enrique Mera Herrera
Michael Adrián Erazo Granizo

Gestión de tecnologías de la información, marco normativo y marco metodológico del control interno de TI en el sector público.

ISBN: 978-9907-0-0579-0

Año: 2025

TOMO I GESTIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN: UNA PERSPECTIVA DEL CONTROL INTERNO EN EL SECTOR PÚBLICO

AUTORES:

BYRON NAPOLEÓN CADENA OLEAS

RAQUEL VIRGINIA COLCHA ORTIZ

WILMER ENRIQUE MERA HERRERA

MICHAEL ADRIÁN ERAZO GRANIZO

GRUPO BLR

Este libro ha sido debidamente examinado y valorado en la modalidad doble par ciego con fin de garantizar la calidad científica.

©Grupo Editorial BLR
Riobamba – Ecuador
Correo: publicaciones@grupoblr.com
https://grupoblr.com/libros-investigo
REPOSITORIO

Cadena, B.,Colcha, R.,Mera, W.,Erazo,M. (2025) Tomo I Gestión de tecnologías de la información: una perspectiva del control interno en el sector público. Grupo Editorial BLR.

ISBN:
978-9907-0-0579-0

FILIACIONES DE LOS AUTORES

Byron Napoleón Cadena Oleas

Escuela Superior Politécnica de Chimborazo

Correo Electrónico: bcadena@espoch.edu.ec

ORCID: https://orcid.org/0000-0002-4535-5265

Raquel Virginia Colcha Ortiz

Escuela Superior Politécnica de Chimborazo

Correo Electrónico: raquel.colcha@espoch.edu.ec

ORCID: https://orcid.org/0000-0002-3252-9158

Wilmer Enrique Mera Herrera

Universidad Nacional de Chimborazo

Correo Electrónico: wilmer.mera@unach.edu.ec

ORCID: https://orcid.org/0009-0006-4484-950X

Michael Adrián Erazo Granizo

Universidad Nacional de Chimborazo

Correo Electrónico: michael.erazo@unach.edu.ec

ORCID: https://orcid.org/0000-0003-0247-1394

GRUPO BLR

PRÓLOGO

La rápida digitalización que está experimentando el sector público ha provocado una profunda transformación en la gestión institucional, posicionando a las Tecnologías de la Información (TI) como una línea estratégica capaz de asegurar la transparencia, la eficiencia y la seguridad de la información. Las instituciones deben responder a nuevos requerimientos funcionales y normativos que exigen tener un control más exacto de sus sistemas, procesos y servicios en tecnologías. La modernización del Estado ecuatoriano, concretamente, pone de manifiesto la necesidad de establecer la gobernanza de las TI como una estrategia que asegure la continuidad y calidad del servicio público.

Este libro, surge como una herramienta importante para la comprensión y análisis de la función tecnológica desde un enfoque global; en su contenido se aborda la vertiente administrativa, la evolución de la gestión de TI y el control interno como elemento de articulación entre la tecnología y la consecución de los objetivos institucionales. El Tomo I presenta unos modelos conceptual y normativo para poder acercarse a la configuración y funcionamiento del ecosistema digital en el ámbito de las entidades públicas.

La obra revisa las relaciones que se establecen entre la gestión tecnológica y el Código de Normas de Control Interno, sobre todo el Subgrupo 410, responsable de regular los procesos informáticos dentro del sector público. En consecuencia, a partir de un análisis exento y depurado, se proceden a revisar el alcance de estas normas, los peligros a mitigar y las evidencias a generar para la obtención de estándares de

auditoría. Así, la lectura permitirá entender el papel del control interno como elemento de fortaleza institucional y pilar de la transparencia. Además, el libro añade un marco metodológico que orienta a las organizaciones sobre cómo evaluar el control interno de TI. Este marco metodológico abarca criterios, etapas, y herramientas que permiten identificar brechas, medir el desempeño tecnológico e implementar acciones para la mejora continua.

El texto también subraya la relevancia del talento humano, la formación digital y la corresponsabilidad de las autoridades, las unidades de control de TI y las auditorías internas. En ese sentido, el libro invita a reforzar el proceso de profesionalización de las áreas de TI y a fomentar la cultura organizacional para lograr el cumplimiento y la mejora continua.

En su conjunto, este Tomo I ofrece una mirada amplia, actual y específica sobre la gestión de la tecnología en el sector público ecuatoriano. Su aporte se sitúa en la cristalización de la teoría, la normativa y la práctica en un documento guía para profesionales de TI, responsables de control interno, tomadores de decisiones, académicos y estudiantes. Así, se espera contribuir a la construcción de instituciones más seguras, más eficientes y más alineadas a las exigencias del gobierno digital del siglo XXI.

ÍNDICE

INTRODUCCIÓN

La evolución de las Tecnologías de la Información ha establecido un nuevo patrón para las técnicas y ejercicios de planificación, implementación y evaluación respecto de las funciones de las instituciones. La digitalización de los trámites administrativos, estandarización de los servicios y la cada vez mayor dependencia respecto de los sistemas informáticos, obligan a las organizaciones a tener estructuras sólidas y metodologías que les permitan una buena gestión de sus recursos tecnológicos. En estas condiciones, el control interno sería una herramienta necesaria para garantizar que los sistemas funcionen de acuerdo con el cumplimiento de los objetivos de las instituciones y el marco normativo que les sea aplicable.

El presente libro se desarrolla con la finalidad de presentar una visión sistemática y argumentada sobre cómo deberían gestionarse las Tecnologías de la Información y de la Comunicación en el sector público, teniendo en cuenta tanto los requerimientos técnicos como las cuestiones asociadas al principio de responsabilidad, integridad y eficiencia. A lo largo de los diferentes capítulos se examina el rol que juegan los procesos de TI en la gestión pública como una materia estratégica, así como también se plantean líneas para evaluar su funcionamiento desde una óptica organizativa y normativa.

Uno de los núcleos temáticos básicos de esta publicación es presentar una comprensión básica de las estructuras, funciones y componentes que configuran la gestión tecnológica, a partir de un estudio de los fundamentos teóricos de la gestión aplicada a los entornos informáticos,

las tendencias actuales de la organización institucional y aquellos componentes que intervienen en el desarrollo, explotación y mantenimiento de los servicios digitales. Desde esta óptica se busca que el lector logre una visión con la que los hábitos de decisión tecnológica sean más autogestionados.

El contenido del presente tomo pone en evidencia igualmente la necesidad de promover una cultura de la organización que le asigne a la tecnología un papel estratégico. Desde esta visión, cabe entender que los procesos informáticos no deben ser segregados, sino que deben ser abordados como una de las partes de un sistema interdependiente que conecta a unidades administrativas, equitaciones técnicas, direcciones y mecanismos de evaluación permanente. A partir de esta se genera una plataforma conceptual y práctica capaz de contribuir al fortalecimiento de la gobernanza institucional.

En cuanto a la parte final, en esta introducción se muestra al lector un texto que combina teoría, análisis y práctica para abordar la complejidad de la gestión de tecnología en el sector público. El objetivo es proporcionar herramientas que permitan no solo interpretar el comportamiento de los sistemas informáticos sino poder aplicar criterios que fomenten la modernización, pero también la eficiencia y la buena administración de los recursos digitales. Este libro se presenta, por tanto, como una guía de referencia para profesionales, académicos y responsables de los procesos tecnológicos que busquen mejorar la capacidad operativa y la capacidad estratégica de las instituciones públicas.

CAPÍTULO I

1 FUNDAMENTOS DE ADMINISTRACIÓN APLICADOS A LAS TECNOLOGÍAS DE LA INFORMACIÓN

En el ámbito del sector público, esta gestión de las tecnologías de la información requiere implantar un adecuado enfoque administrativo que permita integrar correctamente los recursos humanos, los recursos tecnológicos y los recursos financieros para la obtención de los fines institucionales; estos fundamentos de administración en TI constituyen la base en función de las políticas, procedimientos y prácticas en TI, llevar a cabo la eficiencia en la administración de TI y asegurar la eficiencia, la transparencia y la seguridad de la operación de los sistemas de información y de sus tecnologías.

En el ámbito ecuatoriano, alcanzar dicho objetivo tiene un sentido particular, tanto por la creciente digitalización de los servicios públicos como por la implantación de plataformas de gobierno y las normas que hay que cumplir, como el Código de Control Interno de la CGE, la Ley Orgánica de la Función Ejecutiva y la Ley de Transparencia y Acceso a la Información Pública, entre otras.

El conocimiento de los fundamentos de esta materia permite saber cómo se articulan, organizan, dirigen y controlan los recursos tecnológicos para que cada una de sus acciones favorezca la eficiencia de la organización, el cumplimiento normativo y la satisfacción de los ciudadanos; y establece los cimientos para llevar a cabo la gobernanza de TI, la gestión de riesgos, la planificación estratégica, la innovación

tecnológica, aspectos todos ellos vitales para la transformación digital del sector público.

Y a partir de la asunción de estos conceptos se entiende la gestión de TI como un, absolutamente, imprescindible para el buen gobierno, la transparencia, la continuidad de las operaciones y la mejora, la mejora de los servicios públicos digitales en el Ecuador.

1.1 Conceptos básicos de la administración aplicada a entornos tecnológicos

La administración aplicada a entornos tecnológicos está constituida por un conjunto de principios, técnicas y herramientas, para poder planear, organizar, dirigir y controlar los recursos tecnológicos de las instituciones públicas. En el caso del Ecuador, esta administración busca que la infraestructura y los sistemas de información, puedan contribuir a los objetivos institucionales, a la atención eficiente a los ciudadanos en general y al cumplimiento normativo.

1.1.1 Principios fundamentales

a) Planeación tecnológica

- Articulación de los objetivos estratégicos del curso propuesto con los Planes Nacionales de Desarrollo y los Planes Operativos Anuales (POA) institucionales.

Ejemplo: El Ministerio de Salud Pública (MSP) de Ecuador ha progresado con los cambios necesarios para implementar sistemas de historia clínica electrónica (HCE), especialmente en hospitales de

atención preferente y hospitales rurales con alta carga asistencial, pero la interoperabilidad y la integración total del sistema también se evidencian como retos significativos.

Estado de la implementación en Ecuador

A partir del año 2013, el Ministerio de Salud Pública (MSP) instaló en funcionamiento el sistema informático que implementaron los gobiernos anteriores denominado Sisalud, para el manejo integral en salud; hasta el año de 2015, Sisalud estaba funcionando en 116 establecimientos (109 centros de atención primaria y 7 hospitales) y a finales del año 2016 en 151 centros médicos estatales.

El propósito que representa esta inclusión es acercarse al 100% del territorio nacional, entregar a los médicos información clínica de manera instantánea y permitir una mejora continua en la calidad y oportunidad de la atención y aunque el país se encuentra en avanzado proceso de implementación de Sisalud, actualmente no existen hospitales, salvo algunos se encuentren aislados y la mayoría de los hospitales privados, que estén interconectados a la interoperabilidad del MSP (Silva et al., 2017).

b) Organización de la unidad de TI

- Se requiere una clara asignación de roles, de responsabilidades, así como de flujos de información internos a fin de articular plataformas virtuales y gestionar la información de los datos del alumnado para que una unidad de TI en educación se organice de forma efectiva.

Ejemplo: El Ministerio de Educación organiza su unidad de TI para coordinar plataformas de educación virtual y gestión de bases de datos estudiantiles.

Distribución de funciones y responsabilidades

- Organización del trabajo: En las situaciones de educación a distancia, la pedagogía que se desarrolla involucra la cooperación de distintos grupos de trabajadores (diseñadores, desarrolladores, tutores, gestores), asignándoles tareas en el diseño, desarrollo y presentación de la información.
- Roles diferenciados: La claridad de los roles (ejemplo, tutores, administradores de plataforma, soporte técnico) afecta de forma adecuada a la calidad y a la buena realización de la prestación de servicios.
- Gestión de usuarios: Las herramientas administrativas permiten asignar permisos, gestionar accesos y gestionar la interacción entre estudiantes y docentes (Liu et al., 2020).

Flujos de información internos

- Integración de sistemas: Plataformas como Moodle y Sakai pueden integrarse con otras plataformas (ej. accesos, herramientas), permitiendo acceder y utilizar herramientas educativas y gestionar datos.
- Comunicación y soporte: Es preciso establecer procesos donde registrar y dar respuesta a las peticiones, la retroalimentación y el soporte, garantizando la traza y la respuesta adecuada a estudiantes y educadores.

- Privacidad y protección de datos: La gestión de la información tiene que contemplar la protección de los datos personales y de la ética en el manejo de la información del alumnado.

Ejemplo de organización

A continuación, se incluye un ejemplo de organización del trabajo en la (Tabla 1), específico para el entorno de la educación a distancia. Esta organización permite representar qué funciones hay asignadas y cómo se fundamenta la operativa de la gestión de las plataformas educativas; la atención al alumnado; la protección de los datos; la coordinación pedagógica.

Tabla 1. Organización del trabajo en entornos de educación a distancia.

Función principal	Rol responsable	Herramientas/Procesos clave
Gestión de plataformas	Administrador de TI	Integración de sistemas, gestión de usuarios
Soporte a usuarios	Mesa de ayuda TI	Registro y seguimiento de solicitudes
Protección de datos	Responsable de datos	Políticas de privacidad, monitoreo
Coordinación pedagógica	Tutor/Docente	Comunicación, feedback, seguimiento

Fuente: *Elaboración propia.*

Cabe resaltar el predominio de que las funciones contengan un rol explícito y unas herramientas o un procedimiento que las marquen, ya

que queda supeditado a ello la operativa, la trazabilidad de las actuaciones y también la calidad de la propia prestación del servicio educativo digital.

c) Dirección y liderazgo

Son fundamentales para coordinar equipos, supervisar proyectos y motivar al personal, especialmente en la implementación de sistemas de votación electrónica en entidades municipales. La literatura reciente destaca la importancia de adaptar estilos de liderazgo, fortalecer la comunicación y considerar factores humanos y contextuales para lograr el éxito en estos proyectos (Krotova et al., 2024).

d) Control y evaluación

La evaluación y el control en el sector público debe ser consensuado en un marco integrado de indicadores de rendimientos, auditorías internas y externas, gestión del riesgo y mediante conseguir el cumplimiento normativo. En el marco de la auditoría de la seguridad de portales web de ministerios, la formulación de/con el uso de códigos de control interno y normas internacionales significan una eficaz vía para el mejorar la gobernanza y/o la protección de la información.

1.2 Evolución de los modelos administrativos

La evolución de los modelos administrativos refleja los cambios históricos, económicos y sociales que han influido en la forma de organizar y gestionar las instituciones. Desde enfoques tradicionales centrados en la jerarquía y el control, se ha transitado hacia modelos más flexibles, orientados a procesos, resultados y personas. Esta

transformación ha permitido mejorar la eficiencia, la transparencia y la capacidad de adaptación de las organizaciones.

1.2.1 Modelo clásico (1980–1999)

- Sistemas aislados, control contable y gestión documental básica.
- Procesos manuales con registros físicos.
- Ejemplo: archivo físico de expedientes civiles y tributarios en ministerios.

1.2.2 Modelo estratégico (2000–2015)

- Implementación del portal Gobierno en Línea, integración de procesos y servicios básicos.
- Interoperabilidad inicial entre ministerios y municipalidades.
- Ejemplo: Ministerio de Finanzas coordina registros contables entre instituciones públicas.

1.2.3 Modelo de transformación digital (2015–actualidad)

- Automatización avanzada, analítica de datos, gestión de riesgos y control interno robusto.
- Ejemplo: Implementación del sistema de gestión de citas médicas en hospitales públicos, con interoperabilidad entre MSP y EPS locales.

1.3 El proceso administrativo en organizaciones públicas digitales ecuatorianas

El sistema administrativo aplicado a las Tecnologías de la Información en el sector público ecuatoriano se organiza y ejecuta en cuatro etapas: planeación, organización, dirección y control, las cuáles quedan interrelacionadas mediante mecanismos de retroalimentación permanente que dejan establecer acciones de corrección y asegurar la eficiencia institucional.

- Planificación: Contiene la fijación de metas estratégicas, la priorización de proyectos tecnológicos y la alineación de las iniciativas con la normatividad vigente y con los planes de desarrollo digital de carácter nacional.
- Organización: Es la designación de los roles técnico, administrativo y de auditoría, así como el diseño de flujos de información y de responsabilidades que aseguren la forma de operar coherente y segura.
- Dirección: Incluye las actividades propias del liderazgo, la supervisión de proyectos y la coordinación de equipos interdisciplinarios a los que se les ha encargado el desarrollo, la gestión del implante y la operación de los sistemas tecnológicos institucionales.
- Control: Encierra la evaluación mediante indicadores, auditorías, gestión de los riegos, verificación del cumplimiento normativo y mecanismos para asegurar la mejora continua.

1.3.1 Aspectos principales y progresos en la autonomía de gasto público

La digitalización ha impactado profundamente los procedimientos administrativos de las instituciones públicas ecuatorianas, posibilitando, a través del uso de plataformas como Gob.ec, SRI en línea, Quipux, y otras similares, la simplificación de trámites, la mejora de la eficacia, el fortalecimiento de la transparencia y la ampliación de la participación ciudadana (Cevallos, 2023).

Asimismo, el país ha reflejado avances evidentes en el índice de Desarrollo de Gobierno Electrónico, que recoge el aumento de la oferta de servicios digitales, la modernización institucional y la incorporación de tecnologías de información, además la incorporación de herramientas como la inteligencia artificial, el big data y los sistemas automatizados permite optimizar procesos de toma de decisiones y mejora la gestión interna de las diversas instituciones públicas (Toapanta et al., 2019).

1.3.2 Retos y desafíos

A pesar de las mejoras, existen importantes retos y desafíos que se acompañan de:

- La brecha de conectividad entre el mundo urbano y el mundo rural, ya que muchas localidades rurales continúan sin un acceso equitativo a los servicios digitales.
- La técnica estatal para la infraestructura de los servicios, que se debe ir reforzando con las crecientes exigencias del mismo.
- La formación del personal público, ya que se hace necesaria una formación continuada para garantizar la implementación de nuevas plataformas.

- La gestión del cambio organizacional, que implica un cambio de las prácticas tradicionales hacia un cambio de cultura hacia una cultura digital.
- La seguridad de la información debido la creciente exposición a ciberataques y la necesidad de políticas de protección de datos.
- La interoperabilidad entre las instituciones, que es una de las condiciones necesarias.
- La adecuación del marco legislativo para poder cimentar los procedimientos de la transformación digital.

1.3.3 Factores críticos de éxito

A fin de comprender cómo se estructuran y coordinan los procesos dentro de los entornos de educación digital, resulta necesario identificar los roles, funciones y herramientas que intervienen en la gestión operativa y pedagógica.

Por ende la Tabla 2, presenta un ejemplo de organización institucional que muestra las funciones principales, los responsables asignados y los procesos o herramientas clave asociados a cada actividad, mismo esquema permite visualizar de manera sintética cómo se distribuyen las responsabilidades y cómo se articulan los distintos actores para garantizar el funcionamiento adecuado de las plataformas, el soporte a usuarios, la protección de datos y la coordinación pedagógica dentro de un sistema educativo mediado por tecnología (Salazar et al., 2025).

Tabla 2. Factores clave y desafíos en la administración pública digital ecuatoriana.

Factor	**Impacto en el proceso administrativo**

Infraestructura tecnológica	Facilita la digitalización, automatización y eficiencia operativa.
Capacitación y gestión del cambio	Permite la adopción adecuada de los sistemas y mejora su uso institucional.
Seguridad de la información	Protege datos sensibles y resguarda los procesos críticos.
Marco regulatorio actualizado	Promueve la innovación, estandarización y protección de derechos.

Fuente: *Elaboración propia.*

1.4 Evolución de la gestión tecnológica en el sector público

La gestión tecnológica en el sector público ecuatoriano ha transitado por tres etapas principales: automatización inicial, digitalización estratégica y transformación digital, cada una con avances y desafíos específicos como se muestra en la Tabla 3 (Villao et al., 2023).

Tabla 3. Etapas de la evolución tecnológica.

Etapa	**Características principales**	**Ejemplos y avances en Ecuador**
Automatización inicial	Sistemas aislados para contabilidad y gestión documental.	Primeros sistemas informáticos en instituciones públicas, sin integración entre áreas.
Digitalización estratégica	Interoperabilidad básica, portales de atención al	Portales como el del IESS para afiliaciones y consultas; inicio de normativas de e-gobierno.

	ciudadano, digitalización de servicios clave.	
Transformación digital	Soluciones en la nube, automatización de procesos, analítica avanzada, control interno y transparencia.	Plataformas integradas, automatización de trámites, uso de analítica y fortalecimiento de TIC.

Fuente: *Elaboración propia.*

1.5 Tendencias contemporáneas en gobernanza, agilidad y transformación digital

La gobernanza de TI, la agilidad organizacional y la transformación digital en el Ecuador, se son pilares centrales para la modernización del Estado, la oferta de servicios públicos de mejor calidad y la respuesta a las necesidades de una ciudadanía cada vez más conectada. En un marco normativo exigente, con una creciente demanda social y con instituciones que, por tradición, han tenido limitaciones en su funcionamiento e institucionalidad, estos tres tópicos constituyen un pilar fundamental para la potenciación de la administración pública.

Las políticas digitales ecuatorianas, la Agenda Digital 2021–2025, los estándares de la Secretaría de Gobierno Digital y las prácticas asumidas en instituciones públicas, evidencian un tránsito hacia modelos de trabajo más ágiles, eficientes y fundamentados en datos. La literatura reciente, incluida la relacionada en este documento, remarcan que Ecuador está en una fase de consolidación, donde la interoperabilidad, la seguridad de la información, la transformación de procesos y la

adopción de marcos internacionales, son las principales vías del desarrollo institucional digital (Vial, 2019).

1.5.1 Gobernanza de TI en el contexto ecuatoriano: Estructuras, políticas y marcos aplicados

La gobernanza de TI en Ecuador se ha fortalecido a partir de lineamientos establecidos por la Presidencia de la República, MINTEL y la Contraloría General del Estado. En este marco, las instituciones deben asegurar que la tecnología responda a los objetivos estratégicos institucionales, cumpla con la normativa vigente y optimice el uso de recursos públicos.

a) Marcos de referencia aplicados en Ecuador

Las instituciones ecuatorianas han incorporado marcos internacionales como:

- **COBIT** para el control interno y la alineación estratégica.
- **ITIL** para mejorar la gestión de servicios tecnológicos en entidades como el Registro Civil, el IESS y el SRI.
- **ISO/IEC 27001** para fortalecer la seguridad de la información, especialmente en sectores críticos como salud, banca pública y educación superior.

Arroyo y Miguel (2020), enfatizan que estos marcos deben ajustarse a las realidades institucionales de cada sector. En Ecuador, esto implica considerar brechas de talento digital, limitaciones presupuestarias y

niveles diversos de madurez tecnológica entre ministerios, GADs e instituciones educativas.

b) Estructuras y comités de gobernanza en Ecuador

Muchas entidades públicas han creado Comités de Tecnologías de la Información, alineados con el Subgrupo 410 de las Normas de Control Interno. Estos comités:

- Priorizan inversiones tecnológicas.
- Evalúan riesgos institucionales.
- Supervisan la ejecución de proyectos estratégicos (por ejemplo, interoperabilidad, automatización documental o plataformas de trámites).
- Establecen KPIs para medir desempeño tecnológico.

Instituciones como el SRI, CNT EP, MSP y el Banco Central cumplen roles ejemplares en gobernanza tecnológica, dado su nivel de digitalización y su dependencia de sistemas complejos.

c) Gobernanza enfocada en riesgos

La Contraloría General del Estado del Ecuador establece la necesidad de controles que garanticen la disponibilidad, integridad y confidencialidad de los datos. Por esta razón, la gobernanza de la tecnología de la información se basa en:

- Gestión de riesgos de tecnologías.

- Controles de la infraestructura crítica.
- Auditorías periódicas según norma nacional.

Sin duda, este aspecto tiene mayor relevancia con la creciente cantidad de ciberamenazas en el sector público del Ecuador.

1.5.2 Agilidad organizacional en las instituciones públicas de Ecuador

Para atender la demanda y necesidades de los ciudadanos y la normativa vigente, la implementación de la agilidad organizacional se ha hecho necesaria y ha sido abordada de buen talante por el sector privado, aunque la adopción de este concepto, en el sector público ecuatoriano, ha ido en aumento, sobre todo en cuanto a los proyectos de innovación y transformación digital.

a) Adopción de metodologías ágiles en Ecuador

Las entidades públicas ecuatorianas como por ejemplo el Ministerio de Educación, el Ministerio de Salud Pública, el Servicio Nacional de Aduanas (SENAE), la Corporación Nacional de Telecomunicaciones (CNT), el Municipio de Quito, el Consejo de la Judicatura han implementado metodologías Scrum, Kanban o marcos híbridos que les han permitido cumplir con el objetivo de hacer delivery de productos digitales en un tiempo razonable (Gavilanes & Merchán, 2022).

b) Factores que impulsan la agilidad en el Estado ecuatoriano

La trama ecuatoriana se caracteriza por unas condiciones que favorecen que la agilidad se convierta en una necesidad:

- Cambios normativos que ocurren con una gran frecuencia (ejemplo de contratación pública o la política digital).
- Crisis sanitarias y emergencias (la pandemia obliga a digitalizar los trámites de forma repentina).
- Demandas sociales que exigen tiempos más cortos para los trámites, sobre todo en las instituciones de atención masiva.
- Innovación propiciada por organismos internacionales (BID, CAF, UNESCO).

c) Retos para la agilidad en Ecuador

Tal y como explica Vasconez et al., (2025), se enumeran retos universales que en Ecuador se ven potenciados:

- Organizaciones jerárquicas rígidas.
- Falta de cultura de la innovación.
- Capacidades digitales muy bajas del sector público.
- Límites presupuestarios.
- Normativas que privilegian el control al instante de sustituir la flexibilidad.

Por lo que la agilidad del Estado debe compatibilizarse con responsabilidad administrativa y cumplimiento normativo.

1.5.3 Transformación digital en Ecuador: Tecnologías emergentes y decisiones basadas en datos

La transformación digital en Ecuador se ha acelerado desde 2018, impulsada por la Agenda Digital y por la necesidad de modernizar procesos internos. Según el análisis de Merchán y Zambrano (2023),

esta transformación es integral y está acompañada de tecnologías emergentes que permiten optimizar la gestión pública.

a) Tecnologías emergentes implementadas en Ecuador

Inteligencia artificial:

- Chatbots del IESS y MIES.
- Análisis de datos en riesgos fiscales del SRI.

Blockchain:

- Custodia de certificados académicos en universidades ecuatorianas.
- Procesos notariales electrónicos.

IoT (Internet de las cosas):

- Sistemas de movilidad inteligente en Quito.
- Gestión de semáforos y seguridad vial.
- Cloud computing:
- Migración de plataformas estatales a nubes híbridas.

Big Data y analítica:

- Plataformas de información del INEC.
- Información georreferenciada para políticas públicas.

b) Impacto de la transformación digital

La digitalización ha permitido:

- Reducir tiempos de atención ciudadana.
- Mejorar la transparencia y trazabilidad de procesos.
- Fortalecer la eficiencia en entidades de alto volumen transaccional.
- Aumentar la capacidad de respuesta ante riesgos y emergencias.

c) Desafíos ecuatorianos en transformación digital

- Brechas de conectividad en zonas rurales.
- Ausencia de infraestructura robusta en ciertos GADs.
- Débil cultura de protección de datos personales.
- Escasez de talento humano capacitado.
- Limitaciones en interoperabilidad interinstitucional.

Por ello, la transformación digital requiere no solo tecnología, sino reformas institucionales y capacitación permanente.

1.6 La gestión de TI como pilar de transparencia y buen gobierno en Ecuador

La administración de Tecnologías de la Información (TI) se ha ido afirmando con base a un compromiso asumido por el Estado en Ecuador para fortalecer la transparencia, el acceso a la información y el ejercicio del buen gobierno. A ello se le suma que las instituciones públicas tienen el reto de gestionar grandes volúmenes de información, automatizar el proceso de gestión y asegurar el acceso de la ciudadanía a información transparente, oportuna y verificable. En este sentido, la administración de TI va más allá de ser una función operativa y, por el contrario, se

convierte en un eje estratégico para prevenir la corrupción, fomentar la rendición de cuentas y la participación ciudadana.

1.6.1 TIC y transparencia en la gestión pública ecuatoriana

La literatura ecuatoriana sostiene que la modernización del Estado es posible gracias al uso intensivo de las TIC, las cuales permiten ampliar la provisión de servicios digitales y ofrecer más garantías de acceso público a la información. Mina et al., (2025), señala que, los portales digitales son indispensables para "transparentar la gestión pública y hacer partícipe al ciudadano de los procesos del Estado". Este enfoque coincide con la mirada internacional de gobierno electrónico, donde digitalizar significa ser un mecanismo para la mejora de la eficacia, reducir intermediarios e ir democratizando el acceso a los servicios.

Ecuador ha promovido el portal único Gob.ec, el sistema de tramitación en línea, los portales de datos abiertos, así como las plataformas sectoriales como SRI en línea, IESS virtual o Quipux. Estas herramientas permiten que el ciudadano consulte información institucional, acceso a servicios y control social sobre el uso de los recursos públicos con el fin de promover el buen gobierno.

Adaptar el uso generalizado en estas plataformas comporta riesgos que pueden comprometer, la privacidad y la protección de datos. Paguay et al., (2025), alerta cómo muchas instituciones ecuatorianas hacen públicas informaciones personales sensibles en situación de precariedad, así como información sobre salud, datos judiciales o de tipo biométrico e incluso datos sobre y de menores de edad. Esto evidencia que la transparencia debe ser balanceada con la protección de datos, lo

que implica una consideración más que importante para llevar a cabo gestión de TI para asegurarlas.

1.6.2 El funcionamiento de la TI para promover la apertura institucional

La TI de la gestión y el gobierno en Ecuador se desarrolla a partir de diferentes mecanismos de apertura institucional:

a) Registro automatizado de las operaciones de carácter público

El registro de trámites, decisiones de la administración pública, los movimientos presupuestarios y los procesos de contratación se realizan en un sistema que garantiza la trazabilidad, evita la intervención manual y facilita las auditorías internas y externas.

b) Publicación de información en portales de instituciones

La LOTAIP hace obligatoria la publicación de información básica sobre los funcionarios públicos, sobre procesos de contratación, sobre procesos de ejecución de contratos y sobre la ejecución presupuestaria. Las instituciones tienen que publicar mensualmente su información, por lo que es posible que la ciudadanía lleve a cabo el seguimiento. El mal uso de esta norma dio lugar a la publicación indiscriminada de datos personales, como reflejan los hallazgos identificados por Paguay et al., (2025), respecto a las más de 77 subcategorías de datos personales accesibles a partir de los sistemas gubernamentales de Ecuador.

c) Auditorías digitales y trazabilidad

La automatización de procesos permite el control estatal de la administración pública. Sistemas como los e-Sigef, Quipux o los de compras públicas permiten reconstruir procesos administrativos que facilitan identificar el cumplimiento de la legalidad, la eficacia o la detección de irregularidades.

d) Canales digitales de participación ciudadana

Las plataformas de consultas, denuncias, formularios en línea o portales de datos abiertos permiten a la ciudadanía participar en las políticas públicas, fiscalizar actuaciones estatales o aportar otros datos.

e) Planes de continuidad operativa

La gestión de la TI está acompañada por protocolos que garantizan la disponibilidad de los sistemas críticos en caso de fallos, catástrofes o ciberataques. Este aspecto es muy relevante en Ecuador, donde entidades como la ANT, el Registro Civil o los municipios han sido objeto de ataques que han paralizado las operaciones a la espera de los servicios durante una o más jornadas.

1.6.3 Beneficios observados en Ecuador

La gestión adecuada de TI aporta beneficios concretos al buen gobierno:

- Reducción de errores y fraudes: la digitalización disminuye la discrecionalidad administrativa y facilita la detección de irregularidades.

- Acceso a información confiable: plataformas como SRI o Registro Civil permiten verificar datos oficiales en línea.
- Participación ciudadana activa: la ciudadanía consulta, denuncia, solicita datos y evalúa la gestión pública.
- Optimización de recursos: la automatización reduce tiempos de atención, costos operativos y duplicidades administrativas.
- Resiliencia institucional ante incidentes tecnológicos: los planes de continuidad permiten mantener operaciones esenciales.

1.6.4 Riesgos y desafíos que la gestión de TI debe afrontar

Los estudios revisados muestran que Ecuador enfrenta retos significativos:

a) Exposición excesiva de datos personales

Paguay et al., (2025), demostraron que 21 instituciones públicas publican datos sin mecanismos adecuados de protección, exponiendo incluso datos de menores de edad y datos sensibles de salud, judiciales o patrimoniales.

b) Brechas de ciberseguridad

Ataques recientes al Registro Civil, ANT, CNT y gobiernos locales muestran debilidades en la infraestructura digital del Estado.

c) Brecha digital y desigualdad territorial

Aunque ha avanzado el acceso a Internet, las zonas rurales aún presentan limitaciones que afectan la adopción de servicios digitales.

d) Débil cultura de seguridad y protección de datos

La población y a veces los propios funcionarios no siempre comprende los riesgos asociados al manejo de información digital.

e) Falta de interoperabilidad plena entre instituciones

La fragmentación de sistemas dificulta el intercambio seguro de información.

CAPÍTULO II

2 ORGANIZACIÓN, GOBERNANZA Y GESTIÓN ESTRATÉGICA DE TI

En la actualidad, la gestión de las Tecnologías de la Información (TI) en el ámbito del sector público ecuatoriano ha asumido un carácter estructural que contribuye a la eficiencia administrativa, la transparencia, la integridad institucional y la calidad de la prestación de servicios. En el área de control interno, la organización, la gobernanza y la planificación estratégica de las TI determinan el nivel de madurez, el potencial de innovación y la debida observancia de los requisitos nacionales e internacionales.

El acelerado proceso de digitalización que proponen la transformación digital, los planes en torno al gobierno electrónico y la puesta en marcha de las normas de control interno han propiciado la necesidad de ir conformando estructuras organizacionales más consistentes, modelos de gobernanza estandarizados y funciones informáticas que contribuyan al cumplimiento de los objetivos institucionales. La gestión estratégica de TI permite no solo garantizar la continuidad operativa, sino que, sobre todo, sostiene la transparencia, la trazabilidad, la rendición de cuentas, en lo que respecta a los principios del buen gobierno en el Ecuador (Mergel, 2019).

2.1 Modelos de estructura organizacional en TI

Las entidades del sector público ecuatoriano cuenta con un diverso número de modelos organizativos para el cumplimiento de la función

tecnológica. Escoger un modelo no es simplemente encontrar su organigrama, sino que es un tema de gobernanza. Se determina por el tamaño institucional, la complejidad del servicio público, el volumen de datos y especialmente el nivel de madurez digital. Las últimas investigaciones de Ecuador muestran que la estructura de la toma de decisiones no coincide siempre con quien tiene la información técnica, existiendo espacios vacíos entre estrategia y ejecución. A continuación, se exponen los modelos que están más de moda en ese momento de acuerdo con la realidad ecuatoriana:

2.1.1 Modelo centralizado (Monarquía del Negocio)

En este modelo, todas las decisiones y operaciones de TI se concentran en una autoridad única.

Descripción: Una Dirección o Coordinación de TI central controla la infraestructura y las políticas. Sin embargo, la evidencia muestra que, en Ecuador, el 73% de las decisiones de inversión en TI son tomadas exclusivamente por altos ejecutivos de negocio (Rectores, Ministros, Gerentes) sin la participación directa de los líderes de TI (Iddrisu & Fuseini, 2025).

Ventajas:

- Mayor estandarización de procedimientos y compras tecnológicas.
- Control estricto sobre la seguridad de la información y la arquitectura empresarial.

Desventajas y riesgos:

- Desconexión Técnica: Aunque centraliza el poder, a menudo quienes deciden carecen de los insumos técnicos necesarios; solo el 12% de quienes toman decisiones en este modelo proveen los insumos de información.
- Cuellos de Botella: Menor flexibilidad ante necesidades específicas de cada área académica o administrativa.

Contexto universitario: En universidades públicas, este modelo suele fallar cuando las autoridades (Rectores/Decanos) no ven a la TI como un activo estratégico, sino operativo, tomando decisiones erróneas sobre hardware o software sin entender la "arquitectura empresarial".

2.1.2 Modelo descentralizado (Enfoque Feudal)

Cada área operativa (o facultad académica) posee su propia capacidad tecnológica. Este modelo se alinea con el arquetipo "Feudal", donde los líderes de unidades de negocio optimizan sus propias necesidades locales.

Descripción: Es común en instituciones donde las unidades tienen presupuestos autónomos. En Ecuador, el modelo feudal es el más dominante para la provisión de insumos de infraestructura (38%) y arquitectura (30%) (Iddrisu & Fuseini, 2025).

Ventajas:

- Respuesta rápida a necesidades departamentales específicas.
- Alta autonomía operativa para facultades o direcciones regionales.

Desventajas y riesgos:

- Silos de Información: Genera duplicidad de recursos y heterogeneidad tecnológica, dificultando la integración de datos institucionales.
- Madurez "Ad-hoc": Fomenta un nivel de madurez bajo (Nivel 1), donde los procesos son intuitivos y dependen de individuos específicos en lugar de procesos estandarizados.

Caso típico: Municipios medianos o universidades donde cada facultad contrata sus propios sistemas de gestión académica o laboratorios, desconectados de la administración central.

2.1.3 Modelo híbrido o federal (Aspiración Estratégica)

Combina la eficiencia central con la flexibilidad local. Se conoce académicamente como el arquetipo "Federal", donde la cúpula directiva (C-level) trabaja en conjunto con los líderes de las unidades de negocio.

Descripción: Existe una unidad central que define la gobernanza y políticas (el "qué" y el "por qué"), mientras que las unidades ejecutan procesos específicos (el "cómo").

La brecha ecuatoriana: A diferencia de los países desarrollados donde el modelo Federal es dominante, en Ecuador es poco común; apenas el 9% de las decisiones de inversión se toman bajo este esquema colaborativo (Iddrisu & Fuseini, 2025).

Ventajas:

- Equilibrio entre economías de escala y flexibilidad local.
- Alineación estratégica: Permite que la TI se integre en el "core" del negocio, facilitando el camino hacia la "Universidad Digital".

Aplicación estratégica: Es el modelo ideal para implementar marcos como COBIT v5 o ISO/IEC 38500, separando claramente la Gobernanza (evaluar, dirigir) de la Gestión (planificar, construir, ejecutar).

Ejemplos: Instituciones como el IESS o universidades multicampus que buscan transitar de una gestión operativa a una gobernanza corporativa de TI.

2.2 Gobernanza de TI como pilar de la gestión estatal

La gobernanza de la tecnología de la información sí fue definida como el conjunto de estructuras, procesos y mecanismos que se crean y se ponen en marcha para garantizar que la tecnología apoye en logro de los objetivos institucionales y se gestione según los estándares de calidad, seguridad y transparencia.

La literatura ecuatoriana más reciente enmarca la gobernanza de TI no solo como una herramienta de soporte a la organización sino como el sistema a través del cual se moviliza el presente y el futuro del uso de la tecnología. En palabras de Amend et al., (2021) , la gobernanza de TI permite concretar los derechos de decisión y las responsabilidades necesarias para alcanzar comportamientos deseables de uso de la TI, llevando a las organizaciones a poder alcanzar beneficios de hasta un 20% más que sus competidores.

En el sector público ecuatoriano, la gobernanza se articula en torno a tres elementos clave:

2.2.1 Alineación estratégica

La tecnología requiere integración (PEI, PAC, POA). La integración técnica estratégica no solamente es la elaboración de un documento burocrático, sino que es el motivo por el cual las TI dejan de ser un centro de gastos para llegar a ser uno de los activos estratégicos del "core" del negocio público.

a) Realidad en Ecuador

Estudios de toma de decisiones en organizaciones ecuatorianas han puesto de manifiesto que el arquetipo dominante es el de "Monarquía del Negocio", en la moda en que un 73% de las decisiones de inversión son tomadas por altos ejecutivos, sin necesariamente contar con los insumos técnicos requeridos (Amend et al., 2021). Esto genera una brecha de su alineación, que comporta inversiones en infraestructuras que no siempre satisfacen las verdaderas necesidades operativas.

b) Imperativo institucional

La alineación es muy importante para universidades y entidades públicas, puesto que, como exponen Valverde y Llorens (2016), si la TI no forma parte del "core" estratégico de una institución pública está “condenada a vivir en el pasado y morir en poco tiempo”. La gobernanza asegura que cada inversión esté justificada técnica y financieramente, para que la TI se convierta en un medio de alcanzar la excelencia en el ámbito académico y administrativo.

2.2.2 Gestión del riesgo tecnológico

El riesgo operario, cibernético, financiero y reputacional debería gestionarse aplicando metodologías de recaudo exhaustivo. El efecto de la falta de gobernanza en el mismo se encuentra ligado a la gobernanza del erario nacional.

a) Mitigación de proyectos fallidos

Las evidencias empíricas registradas en el Ecuador demuestran que han existido inversiones fracasadas en el área de las TI, las cuales se caracterizaban por la infraestructura considerada como inútil o por proyectos cancelados antes de su inicio y cuya razón era la de una gobernanza mala (Martínez, 2022). Por consiguiente, la gestión del riesgo (lo que podría ser la gobernanza del riesgo), permite describir y comunicar la tolerancia al riesgo de la misma en marcos de gobernabilidad como el COBIT v5 (concretamente el proceso de gobernanza EDM03: Asegurar la optimización del riesgo).

b) Continuidad y seguridad.

Las auditorías de TI y el control interno no deberían ser específicas a la seguridad de la información, sino que deberían recaer en la protección del valor. De una forma paralela, en un entorno donde la penetración del Internet y la dependencia de las tecnologías digitales van en aumento, la protección de los activos en los marcos de decisión establecidos es imprescindible con el objetivo de evitar pérdidas de competitividad y recursos humanos.

2.2.3 Cumplimiento normativo en la gobernanza de TI pública

El hecho de que el cumplimiento normativo en la gestión de tecnologías de la información (TI) en el sector público es fundamental para que se tengan garantías de protección de datos, de transparencia, de continuidad operativa, de rendición de cuentas. La observancia de la Ley Nacional y de los estándares internacionales y la gobernanza de TI sería clave en el combate contra la corrupción y en la mejora de la eficiencia del Estado.

a) Los marcos legales y normativos

Hacen referencia a ley como la Ley Orgánica de Protección de Datos Personales, Ley de Transparencia y Acceso a la Información Pública, regulaciones de los organismos como la Contraloría General del Estado, acuerdos ministeriales sobre incremento de la infraestructura digital y sobre Seguridad, junto a normas INEN y estándares internacionales como ISO 27001, ISO 20000, COBIT, etc. determinaban el marco de la gestión segura y eficiente de la información (Núñez & Pérez, 2022).

b) La gobernanza de TI y el cumplimiento de la legalidad

La gobernanza de TI positiva efectivamente expondría el vínculo entre la cultura del cumplimiento, la mejora de la calidad del servicio, la transparencia y la rendición de cuentas. La aplicación de los marcos COBIT, ITIL e ISO/IEC 20000 permitía alinear la TI y los objetivos organizacionales, gestionar riesgos, asegurar la trazabilidad y el cumplimiento normativo, el cual era fundamental para asegurar la continuidad operativa y la corrupción (Sofyani et al., 2020).

c) Impacto en la transparencia y lucha contra la corrupción

La aplicación de la e-Gobierno bajo marcos normativos solidos serían limitadas hasta que se redujese la discrecionales a la máxima expresión, un aumento en el acceso a actos de corrupción por parte de la ciudadanía, el fortalecimiento de la comunicación entre las partes, y el empoderamiento en el acceso ciudadano a la rendición de cuentas (Sofyani et al., 2020). Sin embargo, la efectividad dependería de la inversión en la infraestructura, de la capacitación, de la integración de las políticas públicas.

d) Retos y tendencias internacionales

Existen retos como es la fragmentación del ordenamiento Jurídico, la falta de interoperabilidad, la necesidad de normalizar estándares internacionales junto con la integración de las tecnologías emergentes (IA, blockchain) para la actualización de marcos de conducción jurídicos, la necesidad de fomentar la cooperación internacional en un mundo interconectado (Khan, 2025).

e) Principales marcos y leyes en cumplimiento normativo de TI

La Tabla 4, sintetiza las normas más relevantes y su nivel de aplicación dentro del contexto público ecuatoriano, permitiendo visualizar su alcance y la importancia que tienen en la configuración de políticas, controles y modelos de gestión de TI.

Tabla 4. Comparación de leyes y estándares clave para el cumplimiento normativo en TI pública.

Ley/Norma/Estándar	Enfoque principal	Aplicación en sector público
Ley Orgánica de Protección de Datos	Protección de datos personales	Alta
Ley de Transparencia	Acceso a información pública	Alta
ISO 27001, ISO 20000, COBIT	Seguridad, gestión y gobernanza de TI	Muy alta
Acuerdos MINTEL, Normas INEN	Infraestructura y seguridad digital	Media-Alta

Fuente: *Elaboración propia.*

2.3 Roles críticos de la función informática

La función informática en el sector público del Ecuador ha adquirido en este decenio una proyección estratégica por la realidad de la transformación digital del Estado, la necesidad de mejorar los servicios de cara a la ciudadanía y la necesidad de una mayor seguridad y gobernanza de la información.

En este sentido, las áreas de tecnologías de la información dejan de ser un simple soporte operativo y pasan a tener un papel fundamental en el planeamiento institucional, la gestión de la información, la interoperabilidad, las infraestructuras de protección crítica y la innovación pública, por ello, comprender estos roles críticos es de gran

importancia para evaluar la madurez digital del sector público ecuatoriano y para localizar esos componentes que permiten garantizar la eficiencia, la transparencia y la continuidad en la operación.

2.3.1 La gobernanza digital y la estrategia digital

a) Descripción / competencias

La función informática tiene que dar el servicio de liderar el establecimiento de la planificación estratégica de TI tal y cómo se ha integrado la Agenda Digital con la Política para la Transformación Digital (2025–2030); definición de la hoja de ruta de servicios digitales, priorización de proyectos transaccionales, coordinación con MINTEL y otras, asegurarse de la alineación con el Plan Nacional de Telecomunicaciones (Macias et al., 2025).

b) Porqué en Ecuador es crítico

En Ecuador el Estado ecuatoriano lanza una agenda nacional (2025–2030), que necesita la coordinación del gobierno, las empresas y la academia; sin una función informática con liderazgo estratégico las iniciativas se quedan fragmentadas, favorecen la ruptura de la interoperabilidad y la reutilización queda debilitada.

2.3.2 Arquitectura, interoperabilidad y gestión de datos

a) Descripción / competencias

Diseñar y gobernar la arquitectura de TI (APIs, catálogos de datos, modelos de datos comunes), habilitar el intercambio seguro de datos entre instituciones (interoperabilidad) y gestionar catálogos/metadatos y

políticas de datos abiertos (Macias et al., 2025). Ello incluye implementar estándares técnicos que habilitan integración y procesos transaccionales entre organismos.

b) Por qué es crítico en Ecuador

Para atender metas de Gobierno abierto y de servicios transaccionales es imprescindible que sean los sistemas el que conversen entre sí: es la función informática la responsable de la plataforma técnica y de datos que habilita la simplificación de trámites y provisión de los servicios digitales integrados.

2.3.3 Seguridad de la información y continuidad operativa

a) Descripción / competencias

Definir y operar el Sistema de Gestión de Seguridad de la Información (SGSI), políticas de seguridad, respuesta a incidentes, planes de continuidad del negocio y pruebas de recuperación ante desastres. Supervisar cumplimiento de normas nacionales y estándares internacionales (p. ej. ISO/IEC 27001) y coordinar con instancias rectoras (Macias et al., 2025).

b) Por qué es crítico en Ecuador

La digitalización amplifica la superficie de riesgo: las entidades públicas custodian datos sensibles (personales, fiscales, de salud). La política pública y documentos oficiales del Ejecutivo insisten en fortalecer la seguridad y la gestión de incidentes como requisito operativo.

2.3.4 Operaciones, infraestructura y conectividad

a) Descripción / competencias

Asegurar disponibilidad y rendimiento de infraestructuras (centros de datos, redes, servicios en la nube, conectividad remota), gestionar contratos con proveedores (incluida provisión de enlaces y servicios en la nube), y optimizar costes operativos mediante modelos híbridos/centrales.

b) Por qué es crítico en Ecuador.

El Plan Nacional de Telecomunicaciones 2024–2025 señala prioridades de conectividad e infraestructura; sin operación robusta la oferta de servicios digitales queda comprometida, afectando la continuidad de trámites y servicios ciudadanos (Mera et al., 2021).

2.3.5 Cumplimiento normativo, privacidad y datos abiertos

a) Descripción / competencias

Garantizar que los sistemas y procesos cumplan normativa de transparencia, protección de datos personales, gobernanza de la información y políticas de datos abiertos; integrar requisitos legales en diseños de sistemas (p. ej. control de acceso, registros de tratamiento, anonimización).

b) Por qué es crítico en Ecuador

La presión por mayor transparencia y protección de derechos digitales obliga a la función informática a traducir el marco legal en controles

técnicos y procesos auditable. Esto reduce riesgos legales y aumenta confianza ciudadana.

2.3.6 Gestión de proyectos, proveedores y compras públicas de TI

a) Descripción / competencias

Dirigir metodologías de gestión de proyectos (agile/PMI), evaluar propuestas, gestionar contratos y gobernar adquisiciones de software/hardware, incluidas licitaciones y contratos de nubes. Supervisar la calidad y cumplimiento de SLAs (Macias et al., 2025).

b) Por qué es crítico en Ecuador

Gran parte del gasto en TI ocurre por adquisiciones puntuales; sin una gestión profesionalizada se multiplican riesgos de sobrecostos, proyectos fallidos y vendor lock-in que frenan la modernización.

2.3.7 Innovación, analítica y uso de tecnologías emergentes

a) Descripción / competencias

Evaluar e introducir tecnologías emergentes (IA, analítica avanzada, IoT, blockchain donde aplique), promover pilotos de valor público, y consolidar capacidades para explotar datos en toma de decisiones. Coordinar laboratorios y alianzas con academia/privados.

b) Por qué es crítico en Ecuador

La Política para la Transformación Digital (2025–2030) demanda investigación, innovación y adopción de tecnologías que mejoren

productividad y servicios; la función informática es la palanca técnica para estas capacidades.

2.3.8 Gestión del talento y capacitación institucional

a) Descripción / competencias

Atraer y retener perfiles TI, diseñar planes de capacitación, certificar competencias, y formalizar cuerpos funcionales con perfiles técnicos y de gobernanza (p. ej. CISO, arquitectos de datos, gestores de servicio) (Mera et al., 2021).

b) Por qué es crítico en Ecuador.

La escala y especialización requerida por la agenda digital exige capacidad interna sólida; sin talento calificado se externaliza know-how y se pierde control sobre activos digitales estratégicos.

2.4 Normativa transversal aplicable a la gestión tecnológica

La gestión de las tecnologías en el Ecuador no se da en un vacío legal, ya que, en la última década, el país ha pasado de una normativa dispersa a un marco jurídico convergente que hace que las áreas de TI deban poner en funcionamiento no solo alineándose a estándares técnicos (como puede ser el ISO) sino a normativa legal que tiene carácter de obligado cumplimiento.

Dicha norma es "transversal" porque afecta a todos los tipos de industria, sean estas la banca y la educación superior. En el siguiente apartado se enumeran los cinco pilares jurídicos que rigen la función informática actual.

2.4.1 Marco constitucional y derechos digitales

La máxima normativa de la gestión tecnológica radica en la Constitución de la República del Ecuador, 2011, la cual fue una de las primeras en la región que consideró el acceso a las tecnologías de la información como un derecho. Ahora bien, para el gestor tecnológico, el artículo crítico será el Art. 66, numeral 19, que establece la protección de los datos personales, es decir, va de un "problema técnico" a "derechos fundamentales" de los cuales cualquier sistema que se pretenda construir deberá responder a la intimidad personal y familiar por expresa disposición constitucional (CONSTITUCION DE LA REPUBLICA DEL ECUADOR, 2011).

2.4.2 Ley Orgánica de Protección de Datos Personales (LOPDP)

Promulgada en 2021, es la norma de mayor efecto práctico en la gestión de TI en la actualidad. La ley obliga a la organización a implementar obligaciones de "responsabilidad demostrada" (accountability).

El gestor tecnológico debe garantizar, por diseño y por defecto, la seguridad de las bases de datos en un servicio de TI. El incumplimiento de esta norma puede derivar en la imposición de multas administrativas de hasta el 1% del volumen de negocio (art. 73); esto ha obligado a las empresas a crear el rol de Delegado de Protección de Datos (DPO) y a redefinir sus arquitecturas de almacenamiento (LEY ORGÁNICA DE PROTECCIÓN & DE DATOS PERSONALES, 2021) .

2.4.3 Ley de comercio electrónico, firmas y mensajes de datos

Afrontada desde 2002 pero renacida de la pandemia, esta ley jugó un papel garante de la validez jurídica de los documentos digitales. El artículo 2 dice textualmente que "el mensaje de datos tendrá el mismo valor que el documento escrito, siempre que quede garantizada su integridad y accesibilidad" (Norma Jurídica Oficial, 2020).

Para la gestión tecnológica, esta es la norma que permite la "Oficina Sin Papeles". Será el área de TI quien se tenga que encargar de poner en funcionamiento sistemas de firma electrónica certificada que garanticen el "no repudio" de las transacciones. Requisito esencial, hoy en día, de la contratación pública y privada.

2.4.4 Código Orgánico Integral Penal (COIP): Delitos informáticos

La gestión de riesgos tecnológicos tiene su interpretación penal en el marco del COIP, siendo que, el gestor de TI debe conocer que la omisión de seguridad no es solo una falta administrativa.

Los artículos 229 al 234 tipifican como delitos la revelación ilegal de bases de datos, la interceptación de la comunicación de datos y el ataque a la integridad de los sistemas informáticos, etc (Salazar et al., 2020). Esto resulta ser vital para la gestión de accesos: un empleado que accede a información no reconocida no únicamente infringe la política de seguridad interna de la entidad, sino que comete un delito.

2.4.5 Ley Orgánica para la Transformación Digital y Audiovisual

Esta es la normativa de referencia vigente (febrero 2023) que establece el camino hacia su modernización. Esta ley modifica diferentes cuerpos normativos para fomentar el uso en la nube de las tecnologías, la

obligación de la facturación electrónica y la administración ágil de los trámites administrativos por medios de interoperabilidad (LEY ORGÁNICA PARA LA TRANSFORMACIÓN DIGITAL Y AUDIOVISUAL, 2023).

Para el área informática, esta ley actúa como habilitador para la contratación de servicios de Cloud Computing público y promueve el uso de firma electrónica en los ámbitos de la Administración y de la empresa privada en general.

CAPÍTULO III

3 PRINCIPIOS FUNDAMENTALES DEL CONTROL INTERNO

En la estructura organizativa contemporánea, el control interno ha dejado de ser un mecanismo meramente sancionador para convertirse en un sistema integral de aseguramiento estratégico. La sostenibilidad de las instituciones, tanto públicas como privadas, depende en gran medida de su capacidad para gestionar adecuadamente los riesgos y garantizar altos niveles de transparencia operativa, lo que fortalece la confianza, mejora la toma de decisiones y contribuye a su continuidad en el tiempo. En este capítulo se presentan las bases teóricas y normativas del control interno, para hacer un análisis de los objetivos, de los roles de los protagonistas y para acercar y homogeneizar los estándares internacionales (COSO, ISO) con la normativa estatal en vigor.

3.1 Conceptualización y objetivos del control interno

El concepto del control interno ha pasado de tener una visión aislada en cuanto a revisión contable hasta llegar a tener una visión sistémica y multidimensional, es decir, al sistema. De acuerdo con el Committee of Sponsoring Organizations of the Treadway Commission (COSO), control interno es aquel proceso llevado a cabo por la junta de administradores, la administración y el resto de personal de una entidad, orientado hacia la consecución de una seguridad razonable en relación con el logro de los objetivos (Landsittel et al., 2013).

Académicamente esta definición se puede descomponer en dos dimensiones básicas:

3.1.1 Proceso dinámico

No es un acontecimiento o un listado de verificación estático; es la sucesión de acciones que permea las actividades operativas de la entidad.

3.1.2 Seguridad razonable

Se da por sentado que ningún sistema puede ser realmente infalible debido a limitaciones inherentes (errores humanos, colusión); el control interno es el intento de reducir, no de eliminar, el riesgo absoluto.

3.2 Responsabilidades de autoridades, servidores y unidades de control

El control interno no es útil sólo porque se encuentre plasmado en manuales, sino que resulta efectivo en tanto esté íntimamente relacionado con las personas implicadas. El paradigama de las tres líneas de defensa (ahora denominado "modelo de las tres líneas", siguiendo la definición del IIA) es el modelo predominante para definir responsabilidades, pero en el contexto de la normativa estatal, este modelo se traduce en la obligación en cuanto a qué deben hacer las autoridades y el cuerpo de servidores.

3.2.1 La máxima autoridad y el nivel directivo

El nivel de responsabilidad llegado el caso del sistema de control interno es de la máxima autoridad de la entidad. Estudios recientes en

gobernanza pública afirman que el llamado "tono en la cima" (tone at the top) es importante, ya que las autoridades deben generar el entorno ético, establecer las políticas de gestión del riesgo y garantizar los recursos necesarios para la implementación de los controles (Peñaherrera et al., 2021). La falta de actuaciones o la omisión en este sentido sería llegar a constituir una de las brechas de la seguridad institucional más significativas.

3.2.2 Servidores o responsables de los procesos (primera línea)

Todo servidor público o empleado operativo es la esencia de la auditoría, un auditor de su propio trabajo. Desde este punto de vista, son responsables de realizar los controles que han sido diseñados con anterioridad (ej. conciliaciones, validaciones y autorizaciones) en el procedimiento habitual para llevar a cabo las operaciones. La normativa estatal en relación con el control interno suele ser lo suficientemente clara para indicar que dicho control corresponde a todos los servidores de la institución, no solo a los auditores.

3.2.3 La Unidad de Auditoría Interna (Tercera línea)

A diferencia de la gestión, la Unidad de Auditoría Interna (UAI) no efectúa controles, sino que verifica de forma imparcial e independiente si los controles están funcionando correctamente. Tiene como función asegurarse por parte de la alta dirección de la organización de que los controles llevados a cabo por la administración están en correcto funcionamiento. En palabras de Quiñónez et al., (2024), la UAI actúa como un consultor estratégico que alerta de las desviaciones antes de

que se conviertan en hallazgos que darían lugar a sanciones por parte de los entes de control externo (Contraloría, entre otros).

3.3 Componentes del control interno según COSO, ISO y normativa estatal

La arquitectura del control interno moderno resulta de la convergencia de marcos internacionales y regulaciones locales.

3.3.1 El marco de control interno COSO 2013

Es el estándar de facto a nivel mundial. Consiste en cinco elementos interrelacionados que deben ser operativos:

- **Entorno de control:** La columna vertebral, la ética, y la estructura organizativa.
- **Evaluación de los riesgos:** El análisis y la información sobre las amenazas que dificultan alcanzar los objetivos.
- **Actividades de control:** Los procedimientos y políticas de control para mitigar los riesgos (ej. segregación de funciones).
- **Información y comunicación:** La recopilación y el intercambio de información necesaria para gestionar y controlar la actividad.
- **Actividades de supervisión:** Las evaluaciones continuas para mantener organismos en funcionamiento.

3.3.2 Normas ISO y complementariedad

Mientras COSO ofrece un marco conceptual, las normas ISO aportan metodologías de implementación específicas. ISO 31000 (Gestión de Riesgos) hace un buen maridaje con el componente referente a

evaluación de riesgos de COSO, dándole concreción tan solo a modo de directrices del riesgo a tratar y monitorizar; así se suma a ISO 37001 (Sistemas de Gestión Antisoborno), la cual da valor al control ético del componente de control interno de COSO. En Journal of Cleaner Production hay investigaciones que demuestran que la integración ISO-COSO como modelo de gobernabilidad, lleva a mejorar la resiliencia organizacional (Fonseca et al., 2021).

3.3.3 Normativa estatal (normas de control interno)

En la esfera pública (en particular en el Ecuador y en la región andina), la Contraloría General del Estado formula Normas de Control Interno (NCI), entendidas, en la praxis, como una voluntad legal del marco COSO. Tienen su carácter normativo obligatorio y transforman los principios teóricos (como la rotación de funciones o la caución) en mandatos legales. La diferencia radica en que, mientras COSO tiene carácter voluntario entre las entidades de derecho privado, la NCI estatal tiene un carácter imperativo y el incumplimiento de los principios establecidos produce responsabilidades administrativas y civiles.

3.4 Relación entre auditoría, riesgo y madurez organizacional

La relación entre auditoría y control interno en la realidad ecuatoriana no se mide como un genérico, sino que es gobernada por la determinación del Nivel de Confianza vigente en el Manual de Auditoría Gubernamental de la Contraloría General del Estado (CGE), y esta determinación es la que realizará el alcance de las pruebas de auditoría. De suyo se refleja la madurez institucional.

3.4.1 Del riesgo inherente al riesgo de control

La normativa ecuatoriana requiere identificar el riesgo previo a la realización de la auditoría. Según indagaciones llevadas a cabo en el ámbito del sector público nacional es inversamente proporcional: mayor madurez de control interno resulta en menor "Riesgo de control", pudiendo la auditoría realizar pruebas de cumplimiento y no exhaustivas de cuentas (pruebas sustantivas) (Merino & Chávez, 2020).

3.4.2 Niveles de madurez: La escala de confianza en Ecuador

La práctica de la auditoría en Ecuador adjudica a las organizaciones tres estados, o niveles de madurez, entendiendo en cada estado cada componente COSO ajustado a la Norma de Control Interno (NCI) (Peña, 2023):

Nivel de confianza bajo (inmaduro): Sucede cuando los controles no existen (cuando se carece de controles) o cuando no se aplican (cuando se aplican controles, pero se aplican mal). La normativa obliga al auditor a hacer Pruebas Sustantivas amplias (revisión de documentos al 100% o con muestras muy grandes) con el objetivo de detectar fraudes o errores; no se puede confiar en el sistema.

Nivel de confianza moderado (en desarrollo): En este punto, los controles existen, pero tienen deficiencias. La auditoría aplica un enfoque mixto.

Nivel de confianza alto (optimizado): La razón por la que se considera 'optimizado' es porque la entidad ajusta su operativa con la de la NCI de la Contraloría. El punto culminante de esta situación es que la auditoría

se reconoce como un proceso de mejora continua, bien en el manejo de las Pruebas de Cumplimiento, bien en el manejo de una gestión de eficiencia que permite reducir tiempos y costes de fiscalización.

3.4.3 Repercusión en la gestión institucional

Investigaciones recientes en Gobiernos Autónomos Descentralizados (GADs) de Ecuador, caso de Soledispa y Rodríguez (2021), indican que aquellos que logran un nivel de confianza "Alto" en cuanto a sus evaluaciones de control interno de su respectivo nivel alcanzan una ejecución presupuestaria de un 30% y disminuyen las observaciones o glosas de las Instituciones de control. Esto demuestra que la madurez del control interno no es únicamente un requisito burocrático, sino un blindaje legal y financiero para las autoridades ecuatorianas.

CAPÍTULO IV

4 CÓDIGO DE NORMAS DE CONTROL INTERNO DE LA CGE (GRUPOS 100–600)

La administración de los recursos públicos en el Ecuador ha pasado de un enfoque exclusivamente burocrático a un modelo de gestión de seguros estratégicos, que en consonancia con criterios internacionales como COSO (Committee of Sponsoring Organizations of the Treadway Commission) modelará jurídicamente la norma de NCI, a partir del Acuerdo No. 004-CG-2023 de la CGE (Cadena, 2023).

El mismo no es estrictamente procedural, dado el carácter obligatorio que tiene para regular la gestión de los titulares, servidores, así como para las personas jurídicas de derecho privado que administran recursos públicos. La literatura académica más reciente enfatiza a su vez la importancia de la aplicación de éstas para prevenir el fraude y mejorar los rendimientos operativos de la administración pública (Vallejo, 2022).

En oposición a las normativas anteriores, como lo fue el derogatorio Acuerdo 039-CG-2009, la normativa del Acuerdo 004-CG-2023 resalta su carácter dinámico y el carácter trasverso de la seguridad de la información, la gestión de riesgos.

4.1 Estructura general del Código de Normas de Control Interno

Para garantizar una aplicación sistemática y evitar ambigüedades en la interpretación, la Contraloría General del Estado ha asignado una jerarquía codificada de forma taxonómica de tal manera que permite a

los auditores, gestores públicos, etc. identificar con rapidez donde discurre el ámbito y el alcance de cada control.

El sistema de codificación está basado en una jerarquía de cinco caracteres (números) que se dividen en dos campos lógicos:

- **Primer campo (tres dígitos):** "Grupo" y "subgrupo", por ejemplo, la serie 400 engloba todas las Actividades de control, mientras que la 410 engloba solamente aquellas que están dedicadas a la Tecnología de la información.
- **Segundo campo (dos dígitos):** Este segundo campo define el título concreto de la norma, de tal forma que el -01 suele vincularse a aspectos organizativos o definitivos.

Con esta estructura jerárquica queda garantizada la "trazabilidad del control", permitiendo que una deficiencia operativa (nivel de título) pueda ser inmediatamente vinculada a una deficiencia sistémica (nivel de grupo). La reglamentación abarca un total de seis grupos básicos que cubren el ciclo de vida de la gestión pública.

4.2 Grupo 100 – Normas Generales

El Grupo 100 define los cimientos legales y filosóficos del sistema. Y no exactamente de los procesos, sino de las condiciones sine qua non para que el control interno pueda ser desarrollado. De manera que se puede comprobar que la debilidad en el Grupo 100 es, de acuerdo con los estudios sobre gobernanza pública en la región andina, el predictor más fuerte sobre la corrupción institucional.

4.2.1 Responsabilidad y rendición de cuentas

La Normativa 100-01 (Control Interno) y 100-03 (Responsables) dan a entender que la función de control no compete solamente a los auditores, sino que corresponde ineludiblemente a los gestores de la entidad. Por su parte, la normativa 100-04 (Rendición de Cuentas) introduce el principio de accountability, exigiendo que los servidores públicos controlen los recursos y, además, rindan cuentas.

En la práctica, eso equivale a explicar que una directiva que omita controles no está incurriendo en una falta administrativa leve, sino en una infracción a la norma general cuya consecuencia puede ser la formación de responsabilidades civiles culposas.

4.3 Grupo 200 – Ambiente de control

El Grupo 200 es el "clima organizacional" o la cultura ética de la organización. Tal y como lo estipula COSO, el componente se puede entender como el conjunto de normas, procesos y estructuras que son la base de la ejecución del control interno.

4.3.1 Integridad y valores éticos (200-01)

Aunque esta norma es la norma clave de los sistemas, la evidencia empírica sugiere que los controles duros (hardware, software, arqueos) son irrelevantes si la cultura organizacional (controles blandos) es flexible (permisiva) con respecto a las desviaciones éticas. La CGE requiere que las entidades concreten códigos de ética y aseguren que la integridad sea un criterio de gestión del talento humano (Cadena, 2023).

4.3.2 Competencia profesional y estructura (200-04, 200-06)

La disposición 200-04 (Estructura Orgánica) y la disposición 200-06 (Competencia Profesional) imponen a las instituciones el deber de diseñar su organigrama en función de la planificación estratégica (y no la creación de puestos de trabajo específicos o burocratización innecesaria). Este tipo de normas complementa y refuerza lo previsto en la normativa 200-09 (Unidad de Auditoría Interna), la cual debe encontrarse estratégicamente posicionada para determinar la eficacia o no del sistema sin perder la independencia correspondiente.

4.4 Grupo 300 – Evaluación de riesgos

El enfoque moderno de la auditoría y la gestión pública es "basado en riesgos". El Grupo 300 obliga a las entidades a dejar de ser reactivas (apagar incendios) para ser preventivas.

4.4.1 Identificación y valoración (300-01, 300-02)

Las normativas obligan a establecer un proceso cíclico de Identificación y la evaluación de los riesgos (300-01). No únicamente por riesgos de tipo financiero, sino también por riesgos tecnológicos, legales, reputacionales. La Valoración de los riesgos (300-02) consiste en determinar la probabilidad y el impacto potencial de los riesgos, es decir, el proceso incluye establecer matrices de riesgo debiendo ser consistentes mediante actualización periódica.

4.4.2 Respuesta y mitigación (300-03, 300-04)

La entidad no puede ser pasiva ante la identificación del riesgo (en caso contrario, caerá en el riesgo de obsolescencia). Por otro lado, la norma 300-03 esboza la necesidad de determinar una respuesta (aceptar, evitar, reducir o compartir el riesgo) y la norma 300-04 demanda la documentación de un Plan de mitigación. En el caso ecuatoriano, los estudios de Prates et al., (2023), muestran que aquellas entidades que fallan en este grupo obtienen índices significativos de glosas y observaciones por parte de la Contraloría.

4.5 Grupo 400 – Actividades de control

Este constituye el grupo más largo y operativo del código. Las Actividades de Control son aquellas acciones, establecidas a través de políticas y procedimientos, que permite que se cumpla lo que la dirección ha determinado que hay que llevar a cabo para controlar o disminuir los riesgos. Su división en subgrupos contiene áreas críticas como la de Administración Financiera (402), la de Tesorería (403) y la de Administración de Bienes (406); pero, por otra parte, en el período asistimos a que el subgrupo 410 (Tecnologías de la Información), pues ha pasado a ser un ítem esencial, dado que transversaliza al resto de los procesos.

4.5.1 Control en tecnologías de la información (Subgrupo 410)

El Acuerdo 004-CG-2023 expresa 17 normas específicas para TIC, entendiendo que la información es el bien más valioso del Estado.

Control en TIC (410-01, 410-02): La unidad de TIC no puede ser considerada como una isla técnica y mucho menos en la medida que se

ejecute una estrategia institucional. La unidad de TIC debe estar supeditada a una Comisión de TIC dirigida por la autoridad máxima para la priorización de inversiones y el inicio de proyectos.

El Plan Estratégico de TIC (410-04): Debe existir el Plan Estratégico de Tecnologías de la Información y Comunicaciones (PETIC) alineado a la estrategia institucional, al Plan Nacional de Desarrollo, etc. El Plan Estratégico de TIC debe justificar la adquisición de hardware o software en función de la generación de valor público y la utilidad de los recursos públicos.

Desarrollo y Adquisición del Software (410-08): Normativa fundamental para evitar el "software fantasma" o el desastre del software. Exige metodologías formales para el desarrollo, la prueba de separado del software en ambientes que no son de producción, que los derechos de autor del software a medida sean de la entidad pública, la entrega del código fuente, etc.

Seguridad y Continuidad (410-11 y 410-12): En el contexto de la amenaza del ciberataque, la norma 410-11 exige el cumplimiento de la Ley de Protección de Datos Personales, la norma 410-12 impone tener un Plan de Contingencias o el Plan de recuperación de desastres en prueba de recuperación ante desastres, limitando que el servicio público quede detenido con cualquier falla.

4.5.2 Controles financieros y administrativos

El énfasis moderno se ha desplazado hacia TIC, sin embargo, las normas 403 (Tesorería) y 405 (Contabilidad) continúan siendo vitales para

asegurar la liquidez y la veracidad de los estados financieros. La "segregación de funciones" (separar el que autoriza, el que ejecuta y el que registra) es un principio transversal que ha sido reiterado tanto en lo que sería la norma general (401-01), como en la norma que se refiere a las TIC (410-03).

4.6 Grupo 500 – Información y Comunicación

Pasada la fase del control interno, este se torna inútil en la medida en que no existe flujo de la información. El Grupo 500 se encarga de que, en el caso de las partes interesadas, los aspectos relevantes sean identificados, captados y comunicados conforme a los aspectos estipulados, en los tiempos incorrectos.

4.7 Grupo 600 – Supervisión

Finalmente, el Grupo 600 cierra el ciclo de calidad (PDCA). Ningún sistema de control es estático; el entorno cambia y los riesgos evolucionan.

- Monitoreo Continuo: Deben ser los responsables de los procesos los que aseguren la correcta implementación de los controles día a día.
- Evaluaciones Independientes: Y aquí aparece la Auditoría Interna y Externa. La norma pide que las deficiencias detectadas a través de la auditoría sean comunicadas a los responsables y que se realicen planes de acción correctivos.
- Monitoreo de TI (410-14): En el ámbito tecnológico, hay que dotar de Acuerdos de Nivel de Servicio (SLA que como se dijo

anteriormente) y métricas de rendimiento que determine si la tecnología que está entregando el valor esperado y que satisface a los usuarios ciudadanos.

CAPÍTULO V

5 INTRODUCCIÓN AL SUBGRUPO 410: NATURALEZA, ALCANCES Y OBJETIVOS

En la estructura del control gubernamental contemporáneo, se puede observar que, en la actualidad, la tecnología no es un mero recurso auxiliar, sino que se halla en un lugar central de la administración pública. El paternalista Acuerdo 004-CG-2023, emanado de la Contraloría General del Estado (CGE), es un ejemplo que demuestra lo que estamos afirmando, en la medida que es la explicación normada de que el Subgrupo 410, "Tecnologías de la Información", constituye el andamiaje jurídico por el que se sientan las bases para los principios de Gobernanza de TI (Tecnologías de la Información) en el sector público ecuatoriano.

El Subgrupo 410 no es simplemente una relación de requerimientos técnicos; es la manifestación jurídica de principios referidos a la Gobernanza de TI, propuesta en el sector público ecuatoriano. La intención es dar solución a la omisión histórica del alineamiento entre la estrategia institucional y la tecnología.

En este sentido, las investigaciones en administración pública de hoy en día en Latinoamérica, como muestran los trabajos de (Flores et al., 2025a), establecen que la falta de alineamiento estratégico entre TI y el negocio es la causa raíz del 60% de las razones de fiasco en los proyectos de modernización estatal. Así, el Subgrupo 410 es el mecanismo de aseguramiento que promulga que la cifra de dinero que se invierte en TI incorporará valor público, disminuirá riesgos cibernéticos y garantizará

la continuidad de la operación que el Estado realiza en el espacio público.

5.1 Vinculación entre control interno y gestión tecnológica

La dirección de inversiones tecnológicas se tipifica como un área de ingenieros, pero las Normas de Control Interno (NCI) han logrado plasmarlo como un nuevo compromiso directivo, el marco normativo establece un vínculo inquebrantable gracias a los tres elementos reguladores: Alineación Estratégica, Transparencia y Legalidad.

5.1.1 La Institucionalización de la Gobernanza de las TI

El control interno tiene la intención de evitar que TI funcione como una "caja negra". La norma exige que la alta dirección participe de forma directa en la toma de decisiones sobre tecnología. Esto coincide con lo que sostiene el estándar internacional ISO/IEC 38500: la obligación de que el uso de las TI recaiga sobre el cuerpo de gobierno de la organización. En el marco de la norma 410-04 se impone la necesidad de preparar un Plan Estratégico de Tecnologías de la Información y Comunicaciones (PETIC).

5.1.2 El Principio de "Seguridad Razonable" en TI

El control interno en el ámbito de TI no pretende conseguir una invulnerabilidad absoluta (lo que, además, resulta técnicamente imposible), sino que intenta transmitir una seguridad razonable para conseguir la salvaguarda del patrimonio digital. Apunta a conseguir controles costo-efectivos. Como -por ejemplo- provee la norma 410-09 sobre adquisiciones, siempre que haya una compra tecnológica debe

haberse hecho a partir de un análisis de costo/beneficio y de un análisis de riesgo, evitando de ese modo las compras por "moda" o por falta de un paradigma operativo, fenómeno académico designado por el término *technological determinism.*

5.2 Riesgos que mitiga el cumplimiento del Subgrupo 410

El conjunto de estas normas sirve como un escudo protector frente a los riesgos relevantes que pueden amenazar la estabilidad del Estado y que se pueden agrupar en cuatro dimensiones:

5.2.1 Riesgos de interrupción operativa y desastres

La organización puede llegar a depender tanto de los sistemas digitales que ante un posible fallo en el Data Center pueda ser incapaz de ofrecer el servicio al ciudadano. La norma 410-12 (Plan de contingencias) permite mitigar este riesgo ya que exige la existencia de planes de continuidad operativa y de planes de recuperación de desastres (DRP) previamente probados. Se establece la obligación de tener centros de cómputo alternos y requerir claramente respaldos de la información confinados en otro lugar.

5.2.2 Riesgos de integridad y falta de fraude

La manipulación de los datos digitales es una de las causas primordiales de corrupción. La norma 410-03 (Segregación de funciones) permite mitigar este tipo de riesgo asegurando que los roles de desarrollo, producción y administración de los usuarios estén separados y que no entren en contacto entre sí. De igual forma, la norma 410-08 obliga a la realización de "pistas de auditoría" (logs) irrefutables en todo desarrollo

de software, lo que permite la trazabilidad forense de cualquier transacción de los datos.

5.2.3 Riesgos legales y de propiedad intelectual

El Estado debe respetar la ley en todo momento, la norma 410-08 protege a la entidad pública frente a litigios por propiedad intelectual obligando a que los derechos de autor del software que sea desarrollado a medida pertenecen a la misma institución y deben ser registrados ante el organismo competente. Igualmente permite reducir el riesgo de "secuestro tecnológico" por parte de los proveedores ya que exige en los contratos que se realice la entrega del código fuente.

5.2.4 Riesgos de obsolescencia e inefectividad

La norma 410-04 permite mitigar el riesgo por la obsolescencia tecnológica no planificada ya que obliga a la existencia de planes operativos que prevean la renovación y actualización de activos.

5.3 Visión general de las 17 normas

El subgrupo 410 se presenta con un total de 17 normas, abarcando el ciclo de vida completo de la tecnología (Planificación -> Construcción -> Operación -> Monitoreo). En las siguientes líneas se presenta una sinopsis técnica agrupada por dominios de gestión:

5.3.1 Dominio de gobernanza y organización (410-01 a 410-05)

Este bloque establece las "reglas del juego". Define la estructura de la unidad de TI, el modo de crear el Comité Estratégico, define la obligación de la segregación de funciones. El punto clave es la

Planificación (410-04), que requiere alinear los proyectos de TI con los objetivos nacionales y a la que suma la definición formal de Políticas y Procedimientos (410-05) para homogeneizar la operación.

5.3.2 Dominio de adquisición y desarrollo (410-07 a 410-09)

Regula cómo la entidad obtiene tecnología.

- **Proyectos (410-07):** Exige una metodología formal (tipo PMBOK o SCRUM adaptado) que contemple el Costo Total de Propiedad (CTP) y contraste de riesgos.
- **Software (410-08):** Establece controles rigurosos para el ciclo de vida del de desarrollo de software (SDLC) implementando ambientes de pruebas separadas a la producción, e incluye criterios formales de aceptación.
- **Infraestructura (410-09):** Regulación de las compras de hardware y de servicios (incluyendo nube), exigiendo Acuerdos de Nivel de Servicio (SLA) y cláusulas de confidencialidad.

5.3.3 Dominio de operación y seguridad (410-06, 410-10 a 410-13)

Es el núcleo operativo diario.

- **Datos (410-06):** Exige formar una arquitectura de información y un diccionario de datos corporativo. Mantenimiento (410-10): norma la gestión de cambios y parches, exigiendo bitácoras y aprobaciones previas.
- **Seguridad (410-11):** Alineamiento con la Ley de Protección de Datos Personales. Contingencia (410-12): Planes de respuesta ante emergencias y continuidad del negocio.

- **Soporte (410-13):** Gestión de incidentes (Mesa de Ayuda) y administración de identidades/accesos.

5.3.4 Dominio de monitoreo y usuario final (410-14 a 410-17)

Cierra el ciclo de calidad y se une con el ciudadano.

- **Monitoreo (410-14):** Definición de indicadores de gestión (KPIs) y reportes a la alta dirección.
- **Servicios web (410-15):** Regulación de portales institucionales e intranet.
- **Capacitación (410-16):** Planificación continua de formación técnica y de usuario.
- **Firmas electrónicas (410-17):** Normativa para la implementación de la identidad digital y validación de documentos electrónicos en el sector público.

CAPÍTULO VI

6 DESARROLLO ANALÍTICO DEL SUBGRUPO 410 – NORMAS DE TECNOLOGÍAS DE LA INFORMACIÓN

La digitalización del sector público pasa de ser un objetivo aspiracional para ser un imperativo estratégico que transforma la relación entre el Estado y la ciudadanía en este nuevo contexto. La importancia del control de las Tecnologías de la Información (TI) como el instrumento de verificación para que la digitalización genere valor público, haga acceder a la información y pueda disminuir los riesgos de la dependencia tecnológica se erige, el Subgrupo 410 de las NCI, que son Normas de Control Interno dictadas por la Contraloría General del Estado, no sólo constituyen un Estado de requisitos, sino que se presentan como la institucionalización de la Gobernanza de TI en el aparato estatal ecuatoriano.

La literatura académica contemporánea sostiene que la eficacia de la administración pública moderna guarda relación directa con su madurez digital. En este sentido (Criado & Garcia, 2019),afirman que la gobernanza digital se refiere a la instauración de disposiciones organizativas, políticas y reglas que orientan y monitorean las TI. Partiendo de esta premisa, en el presente capítulo se desarrolla un análisis exegético y técnico de las 17 normas del subgrupo, explicitando los edificios normativos, funcional y de continuidad del control.

6.1 Norma 410-01 Organización de la unidad de tecnologías de la información

La primera regla del subgrupo asienta los fundamentos básicos que dan como resultado la estructuración de la gestión tecnológica. Su principio básico dice que la tecnología no puede gestionarse de una forma dispersa o a la improvisada; esta tiene que contar con una unidad formalmente constituida, situada en el organigrama y también dotada de los recursos necesarios para llevar a cabo su misión.

6.1.1 Propósito de la norma: Criterios de diseño organizacional

El propósito de la norma 410-01 trasciende la simple creación de un departamento de "sistemas". Su objetivo teleológico es asegurar la alineación estratégica entre las TI y los objetivos institucionales. En la administración pública, la estructura debe seguir a la estrategia; por tanto, la Unidad de TI debe diseñarse no como un centro de costos o soporte reactivo, sino como un socio estratégico capaz de habilitar nuevos modelos de gestión.

Desde la perspectiva del diseño organizacional, la literatura sugiere adoptar modelos que eviten el aislamiento técnico. Según (Weill & Ross, 2004), en su obra seminal sobre gobernanza de TI, la ubicación jerárquica del CIO (Chief Information Officer) o Director de Tecnología es un predictor del éxito en la generación de valor. La norma exige que la unidad esté posicionada en un nivel que le permita "efectuar actividades de asesoría y apoyo a la alta dirección". Esto implica que el diseño organizacional debe garantizar:

- Independencia operativa: Para tomar decisiones técnicas sin conflictos de interés con las áreas usuarias.

- Capacidad de influencia: Acceso directo a la Máxima Autoridad para la toma de decisiones presupuestarias y estratégicas.
- Transversalidad: Capacidad de interactuar horizontalmente con todas las direcciones de la entidad.

6.1.2 Recursos humanos requeridos

La tecnología por sí sola, respecto a su utilización y gestión, es inerte sin el personal que la gestione adaptándose a tan sólo las condiciones del entorno. La norma hace énfasis a la proporcionalidad en el tipo de personal que ha de existir en la organización o en su generalidad. En el sector público, y en este contexto, resulta muy difícil conseguir una política de recursos humanos adecuada a eso.

El marco de referencia e-CF (European e-Competence Framework) propone que una unidad de TI contemporánea ha de tener suficiente mezcla de competencias técnicas y habilidades blandas (gestión, comunicación, negociación). Aun así, se necesita un gran análisis para llegar a la norma 410-01 a partir de:

- **Cantidad:** Dotaciones de personal en función de la carga de trabajo, del número de usuarios, de la complejidad de la infraestructura, del volumen de proyectos.
- **Calidad (Perfiles):** No basta tener programadores o técnicos de soporte. Hay necesidades de perfiles de gestión de proyectos, de arquitectura de software, de seguridad de la información (dependientes, independientemente funcionales) y de analistas de datos.

Investigaciones en la región andina afirman que la escasez de personal calificado es la razón más frecuente de las faltas de controles internos de TI (Flores et al., 2025). Esa es la razón por la que la realización de esta norma exige un compromiso a largo plazo por la formación y la mejora profesional del personal.

6.1.3 Funciones mínimas de la unidad de TI

La norma establece un repertorio de funciones esenciales que deben estar debidamente registradas en el Estatuto Orgánico por Procesos correspondiente de la entidad. Estas funciones se pueden clasificar en tres áreas, de acuerdo con el modelo ITIL:

- La parte de estrategia y diseño (Plan): Elaboración del Plan Estratégico de TI (PETIC), definición de arquitecturas tecnológicas y políticas de uso. La unidad debe ser prospectiva y podría anticipar necesidades institucionales.
- La sección de transición y operación (Run): Gestión de la infraestructura (servidores, redes), gestión de las bases de datos, y soporte técnico a usuarios (Mesa de Ayuda); esta es la parte más visible y crítica para la continuidad del negocio.
- La parte de mejora continua (Monitor): Evaluación del desempeño de los servicios, gestión de los niveles de servicio (SLA) y optimización de los recursos.

Es importante destacar que la norma sugiere que es conveniente separar la función de Seguridad de la Información. La unidad de TI implementa los controles de seguridad, pero la definición de las políticas, así como la auditoría de cumplimiento deben recaer en un Oficial de Seguridad

de la Información (CISO) independiente, de esta manera se garantiza un esquema de pesos y contrapesos adecuado (ISACA, 2019).

6.1.4 Relación con otras áreas institucionales

La Unidad de TI no actúa en un vacío. La norma 410-01 establece la obligación de mantener debida relación de coordinación con las áreas de generación de valor y de soporte. Esta relación debe ser de cliente-proveedor interno formalizada en acuerdos de nivel de servicio (ANS).

- Con la Alta Dirección: La relación es de asesoría para la innovación y la transformación digital.
- Con Planificación: Para asegurar que los proyectos tecnológicos se reporten dentro del POA, estén alineados a este y cuenten con presupuesto.
- Con Talento Humano: Para la gestión del cambio organizacional que implicará la puesta en funcionamiento de nuevos sistemas.
- Con Jurídico: Para la gestión de la contratación y control de contratos tecnológicos, y del cumplimiento de normativas como la Ley de Protección de Datos Personales.

La falta de relaciones coordinadas con estas áreas de la organización se traduce en el fenómeno “Shadow IT”, por el cual las unidades usuarias adquieren y despliegan tecnología sin condiciones para que la unidad técnica la controle, estandarice, y minimice riesgos de seguridad e incompatibilidad tecnológica.

6.1.5 Riesgos por incumplimiento

La violación de la norma 410-01 pone en peligro a la entidad por los riesgos estructurales que puede correr e incluso su misión. Los más relevantes son los siguientes:

- Riesgo de ineficiencia operativa: La intervención de una unidad mal configurada o con personal especializado no va a ofrecer respuestas ante los incidentes, lo que provocará paradas muy largas en el servicio que se ofrece a los ciudadanos.
- Riesgo de no-alineación estratégica: En ausencia de liderazgo que permita la adecuada toma de posiciones, las inversiones en TI se realizan por pura inercia organizativa y/o por moda tecnológica, por lo que se malgastan recursos públicos en herramientas que no ofrecen respuesta a problemas reales.
- Dependencia de terceras personas: La escasez de personal interno disponible para afrontar las TI durante muchas horas harán que las organizaciones opten por la excesiva tercerización, perdiendo el control del conocimiento de la organización e incluso generando dependencia de terceros.

6.2 Norma 410-02 Comité de tecnologías de la información y comunicaciones

Mientras la norma 410-01 regula la parte operativa y táctico, la norma 410-02 da carta de naturaleza la Gobernanza de TI al nivel más alto. El nacimiento del Comité de Tecnologías de la Información y Comunicaciones (CTIC), es el resultado de necesitar colegiar las decisiones tecnológicas, para que las decisiones no queden en manos de

una sola persona, sino que sean consensuadas y que respondan a la visión corporativa.

6.2.1 Objetivos del comité

El objetivo prioritario del CTIC consiste en llevar a cabo el gobierno de las TI. El funcionamiento de este gobierno de TI incluye tres tareas primordiales que corresponden con la evaluación, dirección y supervisión, según el estándar normativo ISO/IEC 38500.

En torno a la propia normativa de la CGE, los objetivos específicos del propio comité quedan fijados conforme a los siguientes enunciados objetivos:

- Priorización de Inversiones: decidir cuáles proyectos ejecutar y cuáles postergar (siendo la base de la propia decisión los criterios relativos a valor público, los criterios de retorno de la inversión - social o económico – y criterios de urgencia);
- Gestión de Riesgos en Alto Nivel: evaluar los riesgos tecnológicos que pueden incidir en el funcionamiento de la institución y aprobar los planes de tratamiento de los mismos;
- Resolución de Conflictos: ejercer la función de mediadores en caso de demandas contradictorias de recursos de distintos ámbitos usuarios.

El propio CTIC transforma así la tecnología de "caja negra", de carácter técnico, a activo estratégico, transparente y gestionado corporativa y colectivamente.

6.2.2 Integración y perfiles de sus miembros

La efectividad del comité depende absolutamente de la capacidad de sus miembros; tomando como base la norma, este debe estar compuesto por titulares de las áreas sustantivas, no por mandos medios y sin poder de decisión. La composición típica recomendada sería la siguiente:

- Máxima autoridad o su delegado: Quien preside el comité y tiene el voto de calidad. Su presencia debería garantizar la validez política a las decisiones.
- Responsable de la unidad de TI: Policía técnica, que elabora las propuestas, los informes y el análisis de viabilidad.
- Responsable de planificación: Asegura el adecuado acoplamiento con el POA y el presupuesto.
- Responsable administrativo/financiero: Valida la disponibilidad de recursos.
- Responsable jurídico: Aclara la legalidad de las adquisiciones y contratos.
- Responsable de comunicación: Gestiona la estrategia de la difusión de nuevos servicios digitales.
- Representantes de áreas misionales: Los "clientes" claves de la tecnología.

Esta composición multidisciplinar asegura una óptica integral y que la toma de decisiones no esté sesgada tecnocráticamente.

6.2.3 Funciones estratégicas y operativas

Aunque el comité tiene un carácter eminentemente estratégico, sus atribuciones se manifiestan en actividades concretas debidamente reglamentadas en el seno del comité. Las principales funciones son las siguientes:

- Aprobación del PETIC: El Comité tiene la función de validar y aprobar el PETIC, antes de su ejecución.
- Monitoreo del portafolio de proyectos: Debe revisar mensualmente la situación de los proyectos críticos (semaforizar su estado), así como las desviaciones presupuestarias o de cronograma.
- Definición de políticas: El Comité se encarga de aprobar las políticas de seguridad de la información, de uso de los recursos y de contingencias que le propone el área técnica.
- Evaluación de adquisiciones de gran volumen: El Comité revisa y autoriza los pliegos de condiciones, para compras de infraestructura o de software de gran volumen.

El Comité debe evitar tareas de microgestión (ej. decidir qué marca de PC comprar) y debe mantenerse en el nivel de Dirección y Control Estratégico.

6.2.4 Frecuencia y documentación de sesiones

La regularidad es un indicador de la salud del gobierno de TI. Un comité que se reúne/convoca anualmente es ineficaz. Las buenas prácticas y la norma recomiendan una periodicidad mínima (ej. trimestral), con sesiones extraordinarias cuando sea necesario.

La «documentación» es la evidencia del control interno. Cada sesión ha de generar:

- Convocatoria formal: Con su orden del día.
- Actas de sesión: Que reflejen los debates, pero especialmente los acuerdos y las decisiones numerados de forma secuencial.
- Seguimiento de compromisos: Una matriz que permita verificar en la sesión siguiente si se cumplieron las disposiciones anteriores.

La ausencia de actas firmadas es una observación recurrente de auditoría que pone de manifiesto una debilidad del ambiente de control.

6.2.5 Alineación de TI con la planificación institucional

El valor supremo que persigue el comité es la Alineación Estratégica. El modelo de alineación estratégica de (Twizeyimana, 2019), es todavía vigente: la estrategia de TI debe derivar de la estrategia de negocio, pero la infraestructura de TI debería habilitar a nuevas formas de hacer los procesos de negocio.

En la práctica del sector público ecuatoriano, esto significa que el comité debe verificar que cada dólar que se invierte en tecnología, debe tener como función la contribución a un objetivo del Plan Nacional de Desarrollo o a una competencia exclusiva de la entidad. El comité debe hacerse la pregunta: "¿Cómo ayuda este proyecto de software a mejorar el servicio al ciudadano o a reducir el tiempo de trámite?". Si esta respuesta no existe, debe ser considerado el proyecto para su rechazo. Esta función de filtro es fundamental para la garantía de la calidad del gasto público.

6.3 Norma 410-03 Segregación de funciones

La segregación de funciones (SoD,) por sus siglas en inglés, Segregation of Duties) constituye el principal principio axioma del control interno. A nivel práctico tecnológico, la aplicación de esta es especialmente crítica ya que los sistemas de información acumulan ingentes volúmenes de información, tanto transacciones como data. La norma 410-03 tiene el propósito de acotar cuando no de minimizar el riesgo de fraude y error humano a través de la delegación de determinadas funciones de las cuales dependen individuos de forma individual de tal manera que una única persona no ostente el control sobre un ciclo de proceso crítico.

6.3.1 Importancia del control en entornos digitales

En el contexto de la administración pública digital, los privilegios concentrados constituyen una vulnerabilidad sistémica. Un "superusuario", con poderes ilimitados, podría (teóricamente) alterar registros, aprobar transacciones o borrar la evidencia de estas acciones sin supervisión alguna. La importancia de la norma 410-03 estriba en la implementación de un sistema de pesos y contrapesos en la tecnología.

La norma garantiza la integridad de la información y de los sistemas puesto que establece que ninguna acción es posible hasta que estas entidades no se hayan ejecutado, pues necesita la participación de cada uno de los roles para firmar para concluir el proceso.

6.3.2 Actividades incompatibles

La normativa establece la obligación de identificar y, en su caso, segregar actividades que, si recaen en una misma persona llevaría a

conflictos de interés. En cuanto a los TI, las incompatibilidades clásicas objeto de auditoría por parte de la Contraloría son las que se exponen a continuación.

- Desarrollo vs. producción: Quien programa, o sea, quien escribe el código no puede tener la facultad de desplegarlo en el entorno productivo, ni tampoco de modificar los datos reales. Esta incompatibilidad es fundamental, pues da lugar a que, si alguien tiene todas esas facultades, podría insertar "puertas traseras" o lógica maliciosa.
- Administración de seguridad vs. administración de sistemas: Quien otorga accesos (Oficial de Seguridad) no puede ser el mismo que administra los servidores o las bases de datos (SysAdmin). De este modo se evita que un administrador se pueda otorgar permisos excesivos a sí mismo sin control.
- Generación vs. autorización de pagos: En sistemas financieros (GRP), el rol que ingresa la nómina o los proveedores no puede ser el mismo que el que aprueba el desembolso electrónico de pagos.

6.3.3 Modelos de segregación por rol

Para aplicar esta norma, las entidades tienen que configurar y hacer uso de modelos de control de acceso (RBAC), la literatura técnica propone la matriz de segregación (Matriz SoD), la cual puede cruzar roles vs. transacciones.

- Roles de ejecución: Usuarios que inician transacciones (ej. Analista de Compras, etc.).

- Roles de autorización: Usuarios que validan (ej. Director Financiero, etc.).
- Roles de custodia: Usuarios que administran el activo digital (ej. Administrador de Base de Datos - DBA, etc.).
- Roles de registro: Usuarios que auditan (ej. Auditor Interno de TI, etc.).

La norma 410-03 hace hincapié en que la descripción de puestos de trabajo haya que documentar de forma opuesta esas limitaciones recalcando que los perfiles técnicos no pueden acumular funciones operativas del negocio (ej. un técnico de TI no tiene acceso funcional a realizar transferencias de banco).

6.3.4 Excepciones y medidas de compensación

En este sentido, en entidades públicas de pequeño tamaño (como por ejemplo los GADs parroquiales) la obligación de contar con determinada segregación de funciones es difícil de respetar, por la falta de personas para asumir los encargos; la norma lo reconoce y permite excepciones, siempre y cuando se establezcan controles de compensación. Los controles de compensación son aquellos controles que operan como una mitigación del riesgo cuando la prevención no es posible. Ejemplos de controles de compensación aceptables son:

- Auditoría de logs intensiva: Cuando un funcionario debe tener acceso tanto al entorno de desarrollo como al entorno de producción debido a una emergencia, de manera intensiva, se debe llevar el registro de su actividad en bitácoras de auditoría,

inalterables, que sean revisadas a diario por un supervisor independiente.

- Rotación de puestos: Cambio periódico de la responsabilidad de las tareas sensibles a fin de evitar la consolidación del esquema de fraude.
- Supervisión directa: Aprobación manual de las transacciones críticas bien por parte de la Máxima Autoridad, por ejemplo.

6.3.5 Riesgos asociados

Si la organización no respeta esa segregación de manera correcta, entonces se expone a algunas situaciones como las siguientes:

- Fraude interno: Por ejemplo, un empleado podría modificar la nómina, desviar dinero de las cuentas de la compañía o robar los inventarios en digital.
- Sabotaje: En esta situación un empleado que tiene acceso total a los sistemas se encuentra en disposición de destruir, a la vez, respaldos y sistemas productivos.
- Errores operativos: Cuando los sistemas cambian sin ser probados, provocan caídas del servicio (es importante decir que nadie más ha validado la acción).

6.4 Norma 410-04 Plan estratégico y operativo de TI

La improvisación es una de las peores enemigas de la eficiencia pública. La norma 410-04 está destinada a obligar a las entidades a gobernar en técnica su futuro, mediante el uso de instrumentos de planificación formal: el Plan Estratégico de Tecnologías de la Información y

Comunicaciones (PETIC) y el Plan Operativo de TI (POTI) de TI. Dichos documentos no son sólo burocracia, son la hoja de ruta que acompaña la inversión a las necesidades ciudadanas.

6.4.1 Objetivos estratégicos de TI

El PETIC tiene que marcar el rumbo que tomará la tecnología de la institución en un horizonte de 3 a 5 años. La propia norma establece que estos objetivos no pueden ser objetivos aislados, han de dar respuesta a preguntas como: ¿Cómo la tecnología ayudará a reducir los tiempos de espera del usuario? ¿Cómo ayudar a incrementar la cobertura de los servicios en las zonas rurales? De acuerdo con marcos como COBIT 2019, los objetivos de las TI han de ser descendidos a partir de los objetivos corporativos. Un ejemplo claro sería que, si la meta institucional es "Cero Papel", es el objetivo estratégico de las TI sería "Implementar un Sistema de Gestión Documental (Quipux) con Firma Electrónica masiva".

6.4.2 Relación con el POA institucional

La desconexión entre el plan técnico y el presupuesto institucional es, por su parte, un motivo habitual de fracaso. La norma establece una estricta vinculación entre ambos: el Plan Operativo de TI (POTI), que expone los proyectos del año, por ejemplo, renovación de servidores o licencias debe estar integrado en el Plan Operativo Anual (POA) de la entidad, lo que garantiza el financiamiento. Para la norma, un proyecto de TI que no está en el POA, es simplemente, administrativamente inexistente. La norma también establece que el presupuesto de TI debe

ser aprobado por la Máxima Autoridad y monitoreado mensualmente para garantizar el gasto.

6.4.3 Indicadores y metas tecnológicas

"Lo que no se controla no se mide". La 410-04 es una norma que promueve la gestión de las TI basada en evidencia. El propio plan ha de incluir indicadores dedesempeño (KPIs) bien definidos.

- De gestión: % de ejecución del presupuesto de TI, % de avance de proyectos.
- De servicio: Disponibilidad de los sistemas (Uptime 99.9%), tiempo medio de
- resolución de incidentes.
- De impacto: Nivel de satisfacción del usuario interno y externo. Estos indicadores permiten al Comité de TI determinar si la estrategia está funcionando o si, por el contrario, hay que cambiarla.

6.4.4 Alineación normativa y presupuestaria

El proyecto o plan debe adecuarse a la superioridad de la norma. En Ecuador, concretamente, esto significa adecuarse a:

- El Plan Nacional de Desarrollo.
- La Política Pública de Transformación Digital emitida por el MINTEL.
- La Ley de Protección de Datos Personales: Desde la perspectiva del presupuesto, la norma prohíbe las compras no planificadas.

Las compras de emergencia (“tecnología bombero”) deben ser la excepción, no la norma, y deben contener la justificación técnica reforzada ante la Contraloría.

6.4.5 Revisión y actualización anual

La evolución de la tecnología es más rápida que la evolución de la propia administración pública. Un plan que fije 5 años de avance estratégico se ha escrito de tal manera que queda obsoleto. La norma plasmada en el paradigma regula la obligación de la revisión periódica. El PETIC y el POTI son así documentos vivos; se ha establecido que cada uno de ellos debe actualizase, por un lado, una vez al año o, por otro lado, cuando se produzcan cambios drásticos, como nuevas leyes, recortes de presupuestos, ciberataques, etc. El cambio permite a la entidad pivotar de forma flexible su propia visión, ya sea migrando a la nube o aplicando cualquier otra decisión que tome, sin tener que hacer una interpretación deficiente de su propio libro de planificación.

6.5 Norma 410-05 Políticas y procedimientos de TI

La gobernanza tecnológica es insuficiente si se fundamenta en la tradición oral o en la "buena voluntad" de los especialistas. La norma 410-05 impone la carga de la formalización operativa, esto es, la responsabilidad de definir, documentar y difundir un corpus normativo interno orientado a regular la conducta de la organización hacia la tecnología. Esta norma se convierte en el "sistema legislativo interno" de la unidad de TI, proporcionando el sustrato legal para la exigibilidad de las acciones y para la aplicación de las sanciones administrativas del caso de incumplimiento.

6.5.1 Tipos de políticas tecnológicas

Dentro de la arquitectura del Documento de TI, los diferentes artefactos no tienen peso equivalente. La norma requiere que la estructura sea jerárquica, desde lo estratégico hasta lo operativo.

- Políticas de alto nivel (Strategic Policies): Es el conjunto de directrices generales para la Alta Dirección que explicitan la postura de la Institución en temas muy significativos como la seguridad de la información, la propiedad de la información y los activos informáticos de uso aceptable.
- Estándares técnicos: Definen las tecnologías que se exigen adoptar obligatoriamente ("se usará sólo base de datos PostgreSQL v14"). La norma 410-05 también establece que debe tenerse en cuenta las certificaciones internacionales y las leyes asociadas.
- Procedimientos específicos: Son las instrucciones con los pasos a seguir. La norma lista áreas obligatorias que deben ser sometidas a reglamentación, resaltando la gestión de inventarios, la generación de backups, la gestión de incidentes y el control de malware.
- Políticas emergentes: El acuerdo reestructura el control interno para abarcar la extensión de las realidades de la sociedad post-Covid 19, exigiendo explícitamente las políticas como el Teletrabajo o la gestión de servicios en la Nube (Cloud Computing), áreas que anteriormente carecían de la reglamentación pertinente.

6.5.2 Procedimientos mínimos requeridos

La norma no permite la discreción sobre lo que debe ser documentado. Tiene previsto un catálogo exhaustivo de procesos que necesitan ser formalizados de forma escrita y la obligación de garantizar la continuidad y la auditoría de los sistemas. Entre los procesos críticos están los siguientes:

- Gestión de accesos: Hay que documentar el ciclo de vida del usuario (altas, bajas y modificaciones). También la gestión de usuarios con privilegios o "críticos", que, por definición, representan el mayor riesgo de seguridad.
- Gestión de logs y trazabilidad: El procedimiento para el registro y revisión de bitácoras (logs) de transacciones es obligatorio. Sin este procedimiento, la informática forense se hace imposible ante un delito informático.
- Gestión de la configuración: Procedimientos para asegurar que el software base y las comunicaciones tienen una configuración segura y estandarizada (harderización), evitando vulnerabilidades herencia de las configuraciones de fábrica
- Administración de proyectos: La norma vincula la gestión operativa y la estratégica y exige procedimientos documentados de administración de proyectos informáticos.

6.5.3 Aprobación, difusión y vigencia

Una política que no ha sido aprobada, es en realidad papel en blanco. La norma 410-05 es muy contundente con respecto a cadena de mando; será la Máxima Autoridad de la entidad la que deberá aprobar las políticas y

procedimientos. Esto provoca que la responsabilidad de TI se eleve hasta la condición institucional. Resulta importante también la difusión una vez aprobada la política; un error muy típico de la administración pública es el de “miedo normativo”: el usuario no puede cumplir con una norma que desconoce. La difusión debe ser evidenciada (correos, actas de capacitación, intranet).

También requiere de la necesidad de actualización, lo cual es especialmente relevante en entornos tecnológicos, ya que la obsolescencia normativa es un riesgo latente (Siponen et al., 2014). Y finalmente, la norma articula el control interno con el régimen disciplinario, pues los incumplimientos son comunicados a Talento Humano para la aplicación de sanciones administrativas.

6.5.4 Auditoría del cumplimiento

La existencia del escrito no asegura su aplicación. La auditoría de cumplimiento comprueba la discrepancia entre "lo escrito" y "lo ejecutado". La norma, por su parte, otorga facultad a la unidad de TI para supervisar y medir todo aquello que constituye regulación. Para el auditor gubernamental, la evidencia se sitúa en la congruencia.

Por ejemplificar. Si la política de respaldos dice que se hacen copias a las 23:00, el auditor va a comprobar los logs del servidor de backups. Si esto no es así, existe el hallazgo de control interno por incumplimiento de procedimiento formalizado.

6.5.5 Riesgos ante ausencia de políticas

La ausencia de políticas explícitas y del uso de políticas predeterminadas para la resolución de incidencias puede dar lugar a una situación de "anarquía operativa", debido a la ausencia de directrices claras. Los principales riesgos asociados a esta circunstancia son:

- Discrecionalidad y error humano: La circunstancia de que no existan procedimientos establecidos para la resolución de incidentes de baja complejidad, como un par de incidencias con la impresora, Tesla Printing o similares, puede generar que cada técnico determine el procedimiento que le parezca más oportuno. La ausencia de procedimientos a seguir puede limitar la capacidad de realización de las tareas y, sobre todo, dejar sin efecto la repetibilidad y en consecuencia la calidad del servicio ofrecido al usuario.
- Indefensión jurídica: En caso de producirse un incidente (ej. caso de fuga de información por parte de un empleado), si la entidad, por no haber realizado la correspondiente política de confidencialidad, no tiene una política de confidencialidad firmada y difundida, le será más difícil, o cuando menos, cuestionable la posibilidad de realizar acciones legales o administrativas hacia la persona responsable.
- Pérdida de conocimiento: La salida de personal clave se traduce en el traslado del know-how, dado que no hay procedimientos establecidos por los cuales adquirir, retener y recuperar el know-how.

6.6 Norma 410-06 Clasificación y arquitectura de la información

En el escenario de la economía digital los datos son el principal activo del sector público. La norma 410-06 propone la gestión de este activo desde el enfoque de la arquitectura empresarial, la oferta que se impone a la tradicional de "almacenes de archivos". Esta norma hace que las entidades que gestionen sus datos pasen a hacerlo de una manera organizada y gobernada (data warehouse) en lugar de hacerlo de una manera caótica (data swamp).

6.6.1 Tipologías de clasificación

No en todos los casos el mismo tipo de información tiene la misma valoración ni demanda el mismo nivel de protección. La norma dispone la obligación de llevar a cabo un proceso de la clasificación de la información generada. Si bien la norma de la CGE es de carácter general, que en la práctica se debe abrogar con la Ley Orgánica de Transparencia y de Acceso a la Información Pública (LOTAIP) y la Ley de Protección de Datos Personales (LOPDP). La literatura sugiere las tipologías de seguridad estándar aplicables en la norma:

- Pública: Información a la que puede acceder libremente cualquiera (ej. nóminas, contratos).
- Confidencial: Datos personales o estratégicos de la información con acceso restringido por ley.
- Interna: Información operativa que no es secreta pero tampoco pública. La norma específica que esta clase de información determina los niveles de seguridad y la propiedad, y evita que se establezcan controles que impliquen un esfuerzo intelectual

extremadamente costoso a información pública, pero no velada frente a datos sensibles.

6.6.2 Arquitectura institucional de datos

La norma introduce una noción muy avanzada que no contempla aún la mayoría de las entidades públicas existentes en los países considerados: el Diccionario de Datos Corporativo. No obstante, dicho concepto no es un documento técnico concebido y utilizado por programadores, sino que se trata de una regla de gobernanza que tiene que ser continuamente actualizado. El diccionario tiene que documentar las siguientes cuestiones:

- Reglas de validación: ¿Qué define un número de cédula válido? ¿Cuáles son los formatos de fecha empleados?
- Controles de integridad: Relaciones entre las entidades para evitar la presencia de datos huérfanos.
- Relaciones sistémicas: Identificar los sistemas o módulos que componen la arquitectura, así como las interacciones que tienen lugar. Para (Imran, 2025), la ausencia de una arquitectura de datos es el principal escollo para alcanzar la interoperabilidad en el gobierno electrónico (e-Government).

6.6.3 Custodia y propiedad de la información

En el entorno de la norma 410-06 hay que incluir la propiedad del dato; en el gobierno de datos (Data Governance) se diferencian entre:

- Propietario del Dato (Data Owner): Generalmente el área de negocio (ej. Talento Humano es dueño de la nómina). Dicta quién puede acceder, etc.
- Custodio del Dato (Data Custodian): Generalmente TI. Responsable técnico y asegurar, respaldar y mantener el dato disponible. Esta distinción tiene interés para establecer la rendición de cuentas. TI no puede decidir si una persona accede a datos de los que no es propietario (es director del servicio técnico); explica las reglas que se han definido por el dueño en la arquitectura de información, pero no las puede imponer.

6.6.4 Integridad, disponibilidad y confidencialidad

La norma establece que deben implementarse medidas que aseguren la disponibilidad, integridad, veracidad y seguridad de los datos.

- Integridad: Comprobar que los datos no han sido alterados indebidamente (ej. hashes o blockchain en los registros públicos).
- Disponibilidad: Que el dato esté disponible por si se lo requiere –especialmente por la ciudadanía, pero también por el funcionario- (conexión con la norma de pautas de contingencias 410-12).
- Veracidad: La calidad del dato en sentido amplio (Data Quality) implica que es un requisito de control interno. Los datos inexactos llevan a decisiones de política pública erróneas.

6.6.5 Relación con modelos de interoperabilidad

La arquitectura de diseño debe proveer una integración de aplicaciones y procesos de forma transparente. Esa es la base de la interoperabilidad.

La norma 410-05, en su numeral 11 se suma a esta postura en la medida en que son convenios los que pueden provocar flujos de información interinstitucional. Por ello, la arquitectura de datos debería ser todo menos un silo. Debería elaborarse bajo unos estándares abiertos (ej. servicios web REST/SOAP, formato JSON/XML) que permitan, por ejemplo, que el sistema del Registro Civil "hable" con el de Hospital Público, fruto del principio de eficiencia administrativa del Estado(Angraini et al., 2019) .

6.7 Norma 410-07 Administración de proyectos tecnológicos

La ejecución de iniciativas tecnológicas de manera improvisada es una de las principales fuentes del despilfarro del gasto de recursos públicos. La norma relativa a la gestión de proyectos de TI 410-07 exige una disciplina obligatoria, que hace que cada iniciativa de TI deje de ser un esfuerzo aislado y se convierta en un proyecto gestionado formalmente, lo que obliga a la Unidad de TI a definir una metodología que garantice la administración de cada uno de los proyectos, tanto de los internos como de aquéllos que ejecutan otras unidades administrativas.

6.7.1 Metodologías (ágiles, tradicionales, híbridas)

La norma no estipula una única metodología, sino que requiere que se defina una. En el ámbito del sector público, la elección de la metodología debe buscar un equilibrio entre la flexibilidad y el control.

- Enfoque predictivo (Waterfall): el más indicado para los proyectos de infraestructura o las adquisiciones en los que el alcance está fijado y los requisitos son precisos desde el principio. La norma

propone etapas secuenciales como inicio, planificación, ejecución, control y cierre.

- Enfoque adaptativo (ágil/Scrum): es el más recomendado para el desarrollo de software, donde la incertidumbre es alta. No obstante, la agilidad no excluye la documentación y la norma exige "entregables, aprobaciones y compromisos formales", o lo que es lo mismo, que incluso en el caso de la más ágil de las metodologías se exija que cada fart sprint proporcione una prueba documental que sea auditable. La literatura académica más reciente habla de que el sector público se orienta hacia modelos híbridos, donde la gestión financiera y contractual se sigue un modelo en cascada (por rigidez legal) mientras que la ejecución técnica se hace ágil (Mergel, 2016).

6.7.2 Gestión del alcance, tiempo y costo

La norma regula explícitamente la "Triple Restricción" del proyecto, siendo:

- Alcance y Justificación: Todo proyecto debe tener su origen en una justificación, escrita y aprobada, en la que conste la naturaleza, la viabilidad, los objetivos y su relación con los demás proyectos institucionales. Esto contribuye al control del Scope Creep.
- Tiempo (Cronograma): La norma exige que exista un cronograma de actividades que permita el seguimiento de dichas actividades, así como la especificación de los responsables y de los recursos del proyecto.

- Coste (CTP): La norma introduce, también, un tema financiero avanzado, como es el Costo Total de Propiedad (CTP), que no exige que la formulación del proyecto contemple únicamente el precio de la compra, sino que contemple el coste de todos los costes directos e indirectos, mantenimiento, formación, operación, consultoría... que se producen a lo largo de la vida útil del activo. Esto es importante para la sostenibilidad financiera del proyecto.

6.7.3 Documentación requerida y estructura de gobernanza

La acertar del proyecto depende de la persona que lo lidere. Es preceptivo resolver una estructura organizativa escrita, explícita en el marco del proyecto, que se denominará el responsable (Sponsor), que ha de ser un servidor que dé lugar a la toma de decisiones y que deje claro que tiene la autoridad precisa para tomar decisiones.

Además de líderes funcionales y líderes tecnológicos, que son, administradores con funciones descritas y con responsabilidades precisas). La documentación es el eje de la auditoría de los proyectos. Se requiere la formalización que debe hacerse mediante "actas o documentos electrónicos legalizados" para el inicio de etapas importantes y para el control de los cambios. La ausencia de acta de constitución (Project Charter) o actas de reunión de seguimiento también constituye un hallazgo de control interno.

6.7.4 Fase de cierre y lecciones aprendidas

No se considera terminado un proyecto porque se haya entregado el producto, sino porque se haya entregado y cerrado administrativamente

lo que establece la norma 410-07, numeral 10, puesto que esta norma exigirá al cierre la aceptación formal, huellas que apliquen pruebas para certificar la calidad del producto y de la finalidad cierta de los objetivos.

La norma también introduce la gestión del conocimiento mediante la etapa de retroalimentación, ya que los riesgos que fueron identificados y evaluados en el transcurso del proyecto (aquellos que pudieron controlarse y cuya desviación se documenta) deberán ser considerados al momento de la planificación de los proyectos que se diseñan en adelante. Lo anterior contribuye a la creación de una cultura de aprendizaje institucional; puesto que si se provoca el aprendizaje institucional se evitará cometer los mismos fallos.

6.7.5 Riesgos frecuentes

El incumplimiento de esta norma expone a la entidad a:

- Proyectos "Elefante Blanco": Inversiones costosas que no generan beneficios porque no se consideró el CTP o la factibilidad real.
- Desviación de recursos: Sin un cronograma y presupuesto monitoreado mediante informes técnico-económicos, los fondos pueden disiparse sin resultados tangibles.
- Falta de calidad: La ausencia de un plan de aseguramiento de calidad aprobado deriva en productos tecnológicos defectuosos que la entidad se ve obligada a aceptar.

6.8 Norma 410-08 Desarrollo, mantenimiento y adquisición de software

El software se convierte en el activo intangible que les da operatividad a los procesos del Estado. La norma 410-08 regula el Ciclo de Vida del Desarrollo de Software (SDLC), fijando controles exigentes en los procesos de construcción propia (in-house) y de adquisición a terceros. La finalidad es asegurar que las aplicaciones resultan eficaces, seguras, auditable y legalmente protegidas.

6.8.1 Ciclo de vida del software institucional

La norma establece que la Unidad de TI haya de regular los procesos mediante una metodología que deberá quedar documentada. El ciclo de vida del proceso tiene que comenzar por la Ingeniería de Requisitos, la identificación, priorización y especificación de los requerimientos, tanto funcionales como técnicos, que sean aprobados formalmente por las unidades usuarias. Otro elemento clave es la incorporación de los controles de aplicación desde el diseño, es decir, los mecanismos que prevengan, detecten y corrijan los errores, preserven la integridad, el control de acceso y los registros de auditoría. Esto es coherente con la norma y se basa en el concepto de la Seguridad desde el Diseño (Security by Design).

6.8.2 Controles de cambios y versiones

El software es algo que es dinámico, pero la modificación del software tiene que estar controlada para evitar la inestabilidad del mismo. La norma claramente especifica:

- Ambientes separados: Las pruebas tienen que realizarse en un ambiente que sea específico y distinto al de producción. La

formalización del pasar a producción requiere la formalización con actas de aceptación de los usuarios.

- Control de versiones: Hay que llevar un control de las respectivas versiones liberadas y mantener una biblioteca de respaldo con las versiones retiradas del uso, es decir, un soporte que garantice la reversibilidad de versiones en caso de un fallo potencialmente crítico.
- Manuales: La elaboración y actualización continua de manuales técnicos, de instalación, de configuración y de usuario es obligatoria.

6.8.3 Desarrollo interno vs. adquisición externa

La norma trata la dualidad de la solución Build vs. Buy (Construir vs. Comprar) a través de controles específicos para cada opción:

- Buy: Ha de estar basada en el portafolio de proyectos priorizados y alineados a las políticas públicas. Los contratos deben ser desarrollados en detalle para garantizar licencias, soporte, mantenimiento y actualización.
- Build (External Development (Software Factory)): Se necesita justificación escrita y autorización. Un aspecto de relevancia de la soberanía tecnológica es la Propiedad Intelectual (PI), los contratos deben establecer que los derechos de autor pueden pertenecer a la entidad contratante y que el contratista debe entregar el código fuente. Esto ayuda a evitar el secuestro tecnológico por parte del proveedor.

6.8.4 Evidencias requeridas en auditoría

Para evidenciar el cumplimiento de la norma 410-08, el auditor solicitará:

- Documentos de Requerimientos: especificaciones funcionales firmadas por el usuario.
- Criterios de Aceptación: especificación concreta de criterios de aceptación para recibir el software.
- Plan de Pruebas y Resultados: Evidencia de que el software ha sido probado (unitarias, integración) antes de pagado y puesto en producción.
- Certificados de Derechos de Autor: certificado de inscripción del software desarrollado a medida en el organismo correspondiente (SENADI en Ecuador).

6.8.5 Riesgos de seguridad en desarrollos propios

Desarrollo de software que comporta riesgos específicos que recoge la norma a evitar:

- Vulnerabilidades del código: La norma impone aplicar estándares internacionales de codificación segura; de otra manera, podría llevar a ataques de inyección SQL o de XSS.
- Falta de trazabilidad: La norma obliga a incorporar pistas de auditoría (logs) de las transacciones habidas; sin esto sería imposible saber quién modificó un dato sensible.

- Interrupción del servicio: La ausencia de una fase de estabilización o de pruebas mal realizadas puede suponer la llegada de colapsos del sistema cuando entra en producción.

6.9 Norma 410-09 Adquisiciones de infraestructura tecnológica

La adquisición de tecnología en el ámbito en el que nos encontramos no es un mero acto comercial, sino que se trata de un proceso técnico-legal que ha de dar respuesta a una necesidad estratégica ya verificada. La norma 410-09 se ocupa de establecer los controles necesarios que eviten la compra de tecnología sobredimensionada, innecesaria o que no tenga cabida en el proceso de compra; regula todo el ciclo del aprovisionamiento, desde la justificación inicial de la compra hasta la disposición final de los residuos tecnológicos.

6.9.1 Planificación de adquisiciones

La norma acepta y prohíbe la improvisación, delimitando que dicho gasto debe ajustarse a los estándares vigentes y debe cumplir con los objetivos de la organización, que necesariamente debe estar en el Plan Estratégico de Tecnologías de la Información y la Comunicación (PETIC) y en el Plan Anual de Contrataciones (PAC) aprobado. El control interno indica que cada compra deba estar soportada por una justificación documentada que refleje el siguiente contenido:

- Planificación de la capacidad (Capacity Planning): Mostrar técnicamente que la capacidad actual es insuficiente.
- Análisis Costo/Beneficio: Valoración financiera de la inversión.

- Provisión de la vida útil: Para evitar la obsolescencia de los recursos, anticipadamente.
- Evaluación de riesgos: Indicar sobre qué amenaza mitiga esta adquisición. Las excepciones a esta planificación no podrán ser decididas desde el área técnica; esta adopción necesita autorización de la máxima autoridad cuya decisión debe estar soportada por la correspondiente justificación técnica.

6.9.2 Estudio de mercado y análisis técnico

La norma establece requisitos concretos para la formalización de los contratos, diferenciando entre bienes (hardware) y servicios.

- Para Hardware: Los contratos deben tener un perfil concreto (marca, modelo, número de serie, capacidades, interfaces), de modo que sea posible hacer el seguimiento exacto entre lo ofertado y lo entregado.
- Para Servicios (SaaS/IaaS): Se requiere la definición de Acuerdos de Nivel de Servicio (SLA) formales. El contrato tiene que detallar aspectos como la seguridad, la confidencialidad y la propiedad de los datos. Un aporte clave de esta norma es el requerimiento de cláusulas de garantías y de multas, asegurando que el Estado tenga formas de resarcirse de incumplimientos producidos por los proveedores.

6.9.3 Estándares mínimos de hardware y comunicaciones

Al no soslayar la tendencia hacia la nube, la norma trata explícitamente el Cloud Computing, y si una entidad optara por tratar, procesar o

almacenar información en sistemas de tercero (nube), dicha entidad tendrá que elaborar el análisis de riesgo y costo/beneficio, que debe ser aprobado por la máxima autoridad, quien también dispondrá las instrucciones necesarias para mitigar el riesgo de Vendor Lock-in (secuestro por proveedor).

En lo sucesivo, la norma establece todas aquellas previsiones que llevan a asegurar la disponibilidad tanto de los programas fuente como de los datos en caso de que el proveedor del servicio se vea obligado a dejar el mercado o a clausurar un contrato, asegurando de esta manera la continuidad de la operativa.

6.9.4 Proceso de evaluación y selección

Por más que la norma del control interno solamente se refiere al control interno técnico, sí se puede considerar que lista algún tipo de relación con uno de los principios de la contratación pública, el cual proviene de la propia regulación de dicha contratación. La dirección de la organización es el sujeto responsable de garantizar el servicio contratado en función del cumplimiento de las obligaciones; esto es que el administrador del contrato ha de tener un perfil técnico que le capacite para auditar métricas de cumplimiento y no solo se ha de tratar de un administrativo que rubrique las facturas (Reis et al., 2020).

6.9.5 Recepción, pruebas y control

El ciclo de vida del activo culmina en el momento de su baja. La norma ya incluye criterios de responsabilidad medioambiental y seguridad de la información en la fase de baja.

- Borrado seguro: Antes de dar de baja un equipo o de finalizar un contrato de cloud, se debe realizar un backup y el borrado seguro (wiping) de la información, para evitar que datos sensibles del Estado queden en discos duros desechados o en servidores ajenos.
- Gestión medioambiental: La disposición final debe cumplir con la normativa medioambiental de gestión de los residuos (RAEE).

6.10 Norma 410-10 Mantenimiento y control de infraestructura tecnológica

Una vez que se ha adquirido la infraestructura, esta pasa a la fase de operación. La norma 410-10 quiere asegurar la disponibilidad, la integridad y el rendimiento de la plataforma tecnológica mediante procedimientos para realización de mantenimiento y control de cambios estandarizados. Es la norma que regula el "día a día" del centro de datos.

6.10.1 Mantenimiento preventivo y correctivo

La norma obliga a abandonar el paradigma reactivo ("reparar cuando se rompe"); debe ser elaborado y ejecutado un plan de mantenimiento preventivo fundamentado en revisiones periódicas y control. Este plan tiene que hacer referencia tanto a hardware (limpieza, revisión eléctrica) como a software (parches, actualizaciones). En el caso de los bienes en garantía, la norma es muy explícita respecto a la eficiencia en el gasto: el mantenimiento deberá ser proporcionado por parte del proveedor a coste cero para la entidad evitando así la duplicidad de pago por soporte.

6.10.2 Inventarios tecnológicos

La falta de control de activos puede dar paso a un alto riesgo de peculado. La normativa al respecto impone la obligación de contar con un inventario actualizado en el cual consta un detallo de sus características, la valoración de la criticidad y la atribución de las personas responsables. Un punto de atención para la auditoría es la conciliación, debe existir una identificación del inventario físico de TI que cruce con el inventario de los registros de activos fijos. Las inconsistencias al respecto tienden a derivar en glosas por bienes desaparecidos. La norma impone que el control sea un control permanente.

6.10.3 Gestión de cambios y liberación de software

La inestabilidad de los sistemas se produce por alteraciones no controladas. La norma define un proceso estricto para la modificación de software e infraestructura:

- Registro y evaluación: cualquier tipo de cambio (de ley, corrección o mejora) debe quedar registrado y evaluado antes de ser aplicado.
- Autorización: los cambios tienen que estar autorizados formalmente de antemano a la implantación.
- Ambientes separados: No se puede desarrollar o probar en producción. Hay que definir ambientes independientes de desarrollo o pruebas, y de producción.
- Control de versiones: Hay que llevar un control estricto de las versiones que entran en producción.

6.10.4 Registros y evidencias técnicas

La norma solicita trazabilidad. El detalle e información de cada una de las modificaciones será registrada en su correspondiente bitácora e informado a los actores relacionados, adjuntando, por supuesto, las evidencias. Dicha exigencia permite conocer responsables si una modificación autorizada "hunde" el servicio.

Por otra parte, cada modificación obligará a realizar la actualización de los manuales técnicos y de usuario, de forma que no se atente contra la realidad de operación que se está llevando a cabo en el sistema y contra la que se tiene en la documentación.

6.10.5 Controles sobre conectividad y seguridad física

Por último, la norma relaciona el mantenimiento con la seguridad, considerando indispensable la necesidad de medidas tanto lógicas como físicas dependiendo de los entornos y recursos a ser salvaguardados. Esto implica el monitorizado y el control del acceso a los racks de servidores, sistemas de climatización y energía ininterrumpida (UPS), apuntando a optar por una infraestructura segura y confiable.

6.11 Norma 410-11 Seguridad de tecnologías de información

La seguridad ha pasado de ser una mera disciplina técnica (configurar firewalls) a convertirse en una función del gobierno corporativo. La norma 410-11, en este sentido, obliga a las entidades públicas a realizar este tránsito desde la "seguridad informática" hasta la "Seguridad de la Información" (SGSI) no solo para la infraestructura, sino también para

proteger la confidencialidad, la integridad y la disponibilidad de los datos ciudadanos, sin importar su formato.

6.11.1 Controles de acceso e identidad digital

La norma también indica que la organización ha de asegurar que unicamente las personas que tienen la autorización accedan a los recursos, alineándose con el principio de Need-to-Know (Necesidad de saber).

- Gestión de identidades: Se debe proporcionar una identificación única a cada usuario (interno o externo). Las cuentas genéricas (por ej. admin, invitado) no están permitidas, ya que la responsabilidad no se puede imputar.
- Autenticación robusta: la norma exige estándares de autenticación. Para la práctica, actualmente implica desplegar Múltiple Factor de Autenticación (MFA) para accesos críticos, incluso para los servicios expuestos a internet o VPNs administrativas.

6.11.2 Seguridad física y lógica

La defensa debe ser a fondo (Defense in Depth).

- Seguridad lógica: Hace alusión a la instalación de controles perimetrales (controles perimetrales, IDS/IPS), redes segmentadas (VLANs) y endurecimiento (hardening) de los servidores y bases de datos. La norma es expresamente clara al requerir protección frente a un malware, pues exige implícitamente utilización de

EDR (Endpoint Detection and Response) centralizados y actualizados.

- Seguridad física: Los centros de datos no pueden ser de acceso libre. La norma 410-05 y 410-11 exigen controles de acceso físico (biometría, tarjetas), sistemas de videovigilancia, sistemas de control ambiental (temperaturas, de detección y supresión de incendios) para proteger el "hierro" donde residen los datos.

6.11.3 Gestión de vulnerabilidades

La norma relaciona la seguridad técnica con el cumplimiento legal.

- Alineación LOPDP: La norma contempla de manera expresa la obligación de cumplir con la legislación en materia de protección de datos personales. Por ende, las entidades están obligadas a llevar a cabo Evaluaciones de Impacto en la Protección de Datos (EIPD) con carácter previo a la puesta en producción de nuevos sistemas.
- Gestión de parches: Las vulnerabilidades conocidas tienen que ser corregidas. La auditoría comprueba si la entidad tiene un procedimiento proactivo de escaneo de vulnerabilidades (hacking ético periódico) y aplica parches de seguridad liberados por los fabricantes en tiempos prudenciales.

6.11.4 Monitoreo y registro de incidentes

La prevención no es suficiente; la capacidad de detección es vital. La norma exige mecanismos de monitoreo. En entidades maduras, esto conlleva la existencia de un SOC, o cuando menos la centralización de

logs (evt. SIEM). El objetivo de ello es la detención de anomalías (evt. un usuario descargando la BBDD completa a las 03:00) y de respuesta (evt. antes de que se consuma la exfiltración).

6.11.5 Evaluaciones de riesgo de seguridad

La seguridad no tiene un carácter estático. La norma dicta que se realicen evaluaciones de riesgos y vulnerabilidades de forma periódica. Esto se enlaza con la norma 300-01, pero con un tratamiento técnico: deben identificarse aquellas amenazas emergentes (Ransomware, Phishing) y evaluarse si los controles son los adecuados para mitigarlas. Según Mullo y Camero (2025), la falta de actualización de las matrices de riesgo es la principal causa de las brechas de seguridad en los municipios ecuatorianos.

6.12 Norma 410-12 Planes de contingencia y continuidad operativa

La resiliencia representa la capacidad que posee una organización para hacer frente a la interrupción de su actividad, esto es, resistir, absorber, recuperarse y adaptarse ante una interrupción del negocio. La norma 410-12 obliga a que el Estado, cuando se le haga necesario, se opondrá a una crisis (que no se detendrá ante una crisis, para usar la terminología de esta norma). Diferencia en la práctica técnica entre lo que es un "Plan de Contingencia" (respuesta inmediata técnica) y un "Plan de Continuidad" (salida degradada del negocio).

6.12.1 Análisis de Impacto Al Negocio (BIA)

Antes de redactar cualquier plan, la organización debe determinar qué es lo que considera fundamental. A pesar de que la norma de la CGE sea

exactamente igual con la buena práctica ISO 22301, esta última obliga a realizar un BIA (Análisis de Impacto al Negocio).

- RTO (Recovery Time Objective): ¿Cuánto tiempo puede estar, sin que esto sea inaceptable, el sistema de facturación sin funcionar?
- RPO (Recovery Point Objective): ¿Cuánta información (minutos/horas) puede llegar a perder la entidad? Estos parámetros técnicos son los que determinarán la inversión a realizar: un RTO de cero exigirá tener centros de datos espejo (activo-activo), mientras que un RTO de 24 horas permite hacer back up en cinta o en nube fría.

6.12.2 Plan de contingencias (Respuesta técnica)

Es un documento táctico para el personal de TI. El procedimiento describe el "PASO A PASO" para recuperar un servicio determinado después de una avería. La norma específica que debe cubrir averías de los equipos, los programas y el personal (National Institute of Standards and Technology (NIST)., 2024). Debe incluir roles críticos y ciertos escenarios (ej. "Procedimiento para caso de fallo del enlace principal de internet"). Para este documento, la confidencialidad es clave; la norma 410-12 especifica que debe cumplir un tratamiento de información confidencial, pues expresa las vulnerabilidades y las rutas de recuperación de la entidad.

6.12.3 Plan de continuidad operativa (Negocio)

Mientras TI realiza la recuperación de los servidores, ¿qué está haciendo la institución? El Plan de Continuidad de Negocio (BCP) se ocupa de

especificar qué hacer si hay que trabajar manualmente o por medios alternos. La norma sugiere la activación de un centro de cómputo alterno propio o, en su defecto, compartido (Data Center Estatal) (Cedergren & Hassel, 2025). Ese tipo de activación garantiza que, si el edificio principal se ve afectado por un siniestro (incendio, terremoto, etc.), los servicios críticos puedan levantarse inmediatamente en una ubicación geográfica diferente.

6.12.4 Pruebas periódicas y simulacros

Un plan que no haya sido ensayado es simplemente una hipótesis. La norma 410-12 lo deja claro: los planes deben ser probados, entrenados y evaluados de manera periódica. Los auditores de la CGE suelen solicitar las actas de los ensayos realizados. Si la entidad cuenta con un plan correcto en papel, pero no lo ha ensayado (ya sea "ensayo de escritorio" o real), estaríamos ante un incumplimiento normativo severo. Las pruebas permiten ajustar tiempos y comprobar si los backups son buenos para realmente ser recuperados.

6.12.5 Recuperación después de incidentes

El ciclo termina justo en el momento en que se vuelve a la normalidad. El Plan de Recuperación de Desastres (DRP) debe contemplar:

- Actividades Previas: Logbooks / Backups al día.
- Durante el desastre: Ejecución de la emergencia.
- Después del desastre: Failback y análisis forense de causas. La norma establece que es necesario designar un comité de crisis y que sus miembros tienen que tener roles específicos para tomar

decisiones durante la emergencia. Se busca evitar el caos de los liderazgos en momentos críticos.

6.13 Norma 410-13 Administración del soporte tecnológico

El usuario final tiene una percepción del valor de la tecnología que depende casi exclusivamente de la calidad de la ayuda recibida. La 410-13 obliga a las entidades públicas a pasar del modelo "bombero informático" (desorganizado y reactivo) a la propuesta de Gestión de Servicios de TI (ITSM) con la intención de garantizar la seguridad, la integridad y la disponibilidad de los recursos mediante procedimientos de operación estandarizados y una ayuda al usuario debida y trazable.

6.13.1 Mesa de ayuda (Service Desk)

La norma sanciona la Mesa de Ayuda o Mesa de Servicios como el SPOC (Single Point of Contact) del usuario con la tecnología. La Mesa de Ayuda no es sólo un número de teléfono para avisar de incidencias, ni tan solo un menú del tipo "en caso de avería contáctenos"; es el mecanismo idóneo a partir del cual transmitir incidencias y peticiones. En términos de los mecanismos de control interno, la Mesa de Ayuda tiene la función de filtrado y control centralizado de la documentación de incidencias y peticiones. Así pues, evita que el usuario en cuestión pueda solicitar el cambio directamente a los programadores (violando la segregación de funciones) y hace que toda solicitud quede correctamente recogida en el sistema. La literatura científica junto con la práctica confirma que la existencia en el sector público de una mesa de ayuda formal mejora el tiempo de inactividad de un 35% (MacLean & Titah, 2023).

6.13.2 Registro de incidentes y requerimientos

La memoria institucional no puede decidirse en función de las personas que participan en ella; la norma exige el tratamiento de los incidentes reportados de forma mediante mecanismos efectivos. Esto supone hacer un uso obligatorio de herramientas de ticketing que permiten clasificar:

- Incidente: interrupción no planificada de un servicio (por e. "no hay internet").
- Requerimiento: lo que se solicita de algo nuevo (por e. "necesito instalar Office"). El ticket registrado da cuenta de los hechos efectuando la acción de solicitar con la fecha, el usuario que reporta el incidente, la prioridad y cómo se resuelve el requerimiento. Sin el ticket, no podemos realizar análisis de causa raíz para la prevención de incidentes.

6.13.3 Tiempos de respuesta y Acuerdos de Nivel de Servicio (SLA)

La norma añade el concepto de Niveles de Servicio. Se deben definir y llevar a cabo niveles de funcionamiento de todos los procesos críticos, basados en las exigencias de los usuarios y las capacidades tecnológicas que realmente se posee, lo que obliga a la entidad a tener que definir Acuerdos de Nivel de Servicio (SLA) internos: "los incidentes críticos están resueltos en 4 horas; los requerimientos normales en 2 días".

La norma indica que se deben realizar revisiones periódicas para determinar si la capacidad existente es o no suficiente para cumplir estos acuerdos, obligando así a realizar una planificación de la capacidad recursiva (Cadena, 2023).

6.13.4 Gestión de Identidades y Accesos (IAM)

En el campo del soporte tecnológico, la norma 410-13 es la que ofrece controles más exigentes en cuanto a la identidad digital, y por lo tanto se añade a la norma de seguridad.

- Identificación única: Se establece la obligación de conceder una única identificación (usuario) para todos los actores, tanto internos como externos y temporales. Así, el hecho de utilizar cuentas compartidas es un hallazgo de auditoría.
- Ciclo de vida de las cuentas: Se efectúa la estandarización de cómo se crean (altas), se modifican y se eliminan (bajas) los usuarios.
- Revisiones periódicas: También se trata de una actividad de control fundamental la revisión periódica de cuentas y privilegios, que tiene que llevar a cabo el dueño del proceso y el administrador de los sistemas. Con ello se busca detectar y eliminar "usuarios fantasmas" (ex-empleados que todavía tienen el acceso activo a las cuentas).

6.13.5 Evaluación del servicio y transparencia al ciudadano

La ayuda no se limita a dar la solución técnica; necesita en primer lugar comunicarse. La norma dice que ha de haber la implementación de mecanismos, preferentemente electrónicos, que pongan en conocimiento de los usuarios el estado de los trámites que inician. Son mecanismos que constituyen un instrumento fundamental para la transparencia administrativa. Hay que tener en cuenta que se tendrá que tener un repositorio en el que recoger todos los diagramas y configuraciones, permitiendo con ello la resolución rápida de

incidencias y la reducción de la dependencia de variable de una determinada persona técnica que tiene el conocimiento.

6.14 Norma 410-14 Monitoreo y evaluación de procesos y servicios de ti

El ciclo de Deming (Planificar-Hacer-Verificar-Actuar) se cierra con la verificación. La norma de la 410-14 insiere el mandato de Gobernanza por medio del Monitoreo. No es suficiente ejecutar proyectos ni brindar soporte: la entidad debe medir si la tecnología se encuentra contribuyendo a la consecución de los objetivos institucionales planificados y si los recursos se están utilizando de forma eficiente.

6.14.1 Indicadores de desempeño (KPIs) y métricas

La norma establece la responsabilidad de establecer indicadores de desempeño, como también métricas del proceso, a partir de las operaciones de la entidad, hallando en estos indicadores ir más allá del técnico como pudiera ser el término '%' de uso de CPU, para ir al negocio. Algunos ejemplos de KPIs alineados a la norma serían:

- Eficacia: Proporción de proyectos de TI entregados en tiempo y presupuesto.
- Eficiencia: Costo medio por transacción digital.
- Calidad: Proporción de disponibilidad de los servicios críticos (Uptime).

Disponer de las métricas citadas permite a la administración "monitorear la gestión y tomar los correctivos que se requieran", lo que permite que las decisiones sean adoptadas a partir de datos y no de las intuiciones.

6.14.2 Marco de trabajo de monitoreo

El monitoreo no debe ser ocasional. La norma hace referencia para figurar la necesidad de "conformar un marco de trabajo de monitoreo" que defina el alcance, su metodología y el proceso. Esto es, institucionalizar rutinas de control, por ejemplo:

- Monitoreo continuo: Herramientas automáticas que supervisan la salud de la infraestructura 24/7.
- Monitoreo periódico: Revisión mensual o trimestral del cumplimiento normativo y del avance de planes. Según (ISACA, 2019), dentro del marco COBIT, el monitoreo es el componente que hace que la dirección esté informada sobre el rendimiento y la conformidad de TI.

6.14.3 Medición de la satisfacción del usuario

La tecnología es un servicio. La norma impone que se definan y se ejecuten procedimientos a fin de poder medir, analizar y mejorar el nivel de satisfacción de los clientes internos y externos. Esto se concreta normalmente con la utilización de encuestas post-atención (una vez finalizado un ticket abierto en la Mesa de Ayuda) o bien mediante encuestas anuales de percepción. El resultado de la medida es asimismo un indicio de la auditoría, lo que prueba que la entidad está escuchando a sus usuarios y persigue mejorar la calidad del servicio público de manera constante.

6.14.4 Reportes y alertas a la alta dirección

El monitoreo de la TI no proporciona ningún valor si la información no alcance a quien decide. La norma 410-14 deja muy por sentado el hecho de que la unidad de TI debe presentar informes de gestión periódicos a la alta dirección.

Estos informes (cuadros de mando o Dashboards) permiten a la máxima autoridad supervisar el cumplimiento de los objetivos planteados. Un buen informe de gestión de TI debe saber traducir el lenguaje técnico a un lenguaje de negocio, y mostrar riesgos, retorno de valor y estado de cumplimiento normativo.

6.14.5 Trazabilidad y evidencias para la mejora

La acción correctiva es el objetivo final del monitoreo. La norma establece que, a partir de los informes, se deben identificar e implantar acciones correctivas y de mejora. Para quien audita, la evidencia no es solo el indicador en rojo, sino el plan de acción que se ha destacado para corregirlo. Si una entidad comunica cada mes que el flujo de disponibilidad es bajo y no documenta ninguna acción correctiva, está incumpliendo el objetivo de la norma de monitoreo.

6.15 Norma 410-15 Portal web, intranet y servicios telemáticos

En la actualidad de la Administración Pública 2.0, el portal institucional ya no puede ser concebido como una simple "vitrina" informativa, sino el acceso universal a todos los servicios al ciudadano. La norma 410-15 regula la administración de los canales digitales de acceso público a los trámites y servicios públicos regulando que la responsabilidad de la Unidad de TI para elaborar las normas, procedimientos e instrucciones

para la instalación, la configuración y la utilización de los canales digitales.

6.15.1 Gestión del portal institucional y servicios telemáticos

La norma establece que la gestión del portal web se efectúe "de acuerdo con los siguientes mandatos legales, siendo uno de los más directos la Ley Orgánica de Transparencia y Acceso a la Información Pública (LOTAIP)". Esto significa que la forma de llevar a cabo el control interno con respecto al Portal se relaciona directamente con la LOTAIP. El auditor comprobará que el portal "existe" pero también debe constatar el cumplimiento con los principios de calidad que citamos a continuación:

- Disponibilidad: El Portal debe estar operativo continuamente en todos sus servicios en un 24/7.
- Integridad: La información publicada no puede ser susceptible de ser manipulada de forma no autorizada (defacement).
- Usabilidad: El portal debe considerar las demandas que tiene el usuario externo e interno.

6.15.2 Publicación de información y desarrollo de aplicaciones

La norma le ordena a la Unidad de TI tener en cuenta el desarrollo de aplicaciones web y/o móviles, los cuales permiten automatizar procesos. La finalidad de esta tecnología es desmaterializar el trámite, esto es, pasar de la fila al clic. Aun así, TI sí debe determinar los flujos de publicación seguros para que, si llega información equivocada, no sea de manera pública.

6.15.3 Accesibilidad y seguridad en servicios expuestos

Al brindar servicios en internet (correo, intranet, portales) se hace mayor la superficie de ataque. La norma solicita la puesta en práctica de procedimientos de configuración seguros (hardening).

También la literatura y estándares como W3C/WCAG (intencionadamente referidos en la cláusula de cumplimiento de la legalidad vigente) obligan a que el contenido de los portales públicos sea accesible para personas discapacitadas. Un portal de la Administración que no sea accesible a lectores de pantallas incumple el principio de accesibilidad universal aplicado al servicio público (Zaitouni et al., 2024).

6.15.4 Servicios en línea e Intranet

La norma regula, además, la Intranet y la utilización del correo electrónico institucional.

- Uso aceptable: Se debe establecer una política clara sobre qué se puede o no transmitir a través de los canales no oficiales.
- Colaboración: Con la Intranet se pretende que la misma sirva como repositorio de conocimiento y de gestión documental interna. Aumentando la eficiencia de la comunicación interna y reduciendo al máximo el uso del papel.

6.16 Norma 410-16 Capacitación en tecnologías de la información

La falta de habilidades digitales se puede considerar como uno de los mayores riesgos operativos del sector público, ya que ninguna

tecnología de vanguardia servirá de nada si el personal no sabe utilizarla. La norma 410-16 nos envía un mensaje de corresponsabilidad que establece que, junto con la Unidad de TI, la Unidad de Talento Humano ha de hacer su trabajo en coordinación.

6.16.1 Detección de necesidades de capacitación

La norma establece que hay que "identificar y documentar las necesidades de formación". Por lo que, en sí, prohíbe la formación "por catálogo" o "la formación sin diagnóstico previo" también, por lo que el plan de formación no puede ser un catálogo de formación que se pide en un plan de formación, sino que tiene que ser un plan de formación que esté derivado de una evaluación de competencias:

- Para el personal técnico: Formación especializada (p. ej., certificación en Oracle, ciberseguridad, gestión de proyectos) necesaria para mantener la infraestructura operativa.
- Para usuarios finales: Formación de la alfabetización digital, uso de los sistemas institucionales (ERP, GRP) y una formación en concienciación sobre la seguridad de la información.

6.16.2 Programas institucionales obligatorios y continuos

La presente norma dice que en el Plan de Capacitación tiene que haber temas obligatorios y continuos, la capacitación no puede ser un evento aislado. Cuando se habla de la seguridad se puede decir, por ejemplo, que la capacitación en "Cómo detectar Phishing" ha de ser recurrente. La falta de este punto en el plan anual es algo que puede ser denunciado

por la Contraloría ya que normalmente los incidentes solicitados por la seguridad suelen ser debidos a errores humanos.

6.16.3 Competencias digitales mínimas y evaluación

El objetivo final es que "el personal utilice adecuadamente las aplicaciones tecnológicas, los servicios y sistemas de información para la ejecución de los procedimientos institucionales". En el marco de control interno se precisa de evidencia de la eficacia de la capacitación: ¿Mejoró la actuación del funcionario tras la formación? Las listas de asistencia no son válidas, y se exige incluso evaluaciones de conocimiento o desempeño virtual tras la capacitación.

6.17 Norma 410-17 Firmas electrónicas en la administración pública

Una de las normas más completas y extensas. Esa es la razón que da cuenta de la importancia jurídica de la identidad digital en el Ecuador. La norma 410-17 define la transición a “Oficina Sin Papeles”, indicando qué ajustes tienen que realizar las entidades para integrar para utilizar la firma electrónica de conformidad con el marco legal. (Ley de Comercio Electrónico).

6.17.1 Validez legal y protocolos de uso

La norma consagra la posibilidad de utilizar la firma electrónica personal de los servidores públicos para el ejercicio de su función pública y para firmar los actos administrativos de su competencia, implicando un cambio en los flujos de trabajo (workflow); debiendo el control interno asegurarse de que existan los sistemas de gestión

documental (Quipux o equivalentes) interconectados con mecanismos de firma acreditados por parte de la ARCOTEL. El principio rector es el de No Repudio, esto es, garantizar que electrónicamente queda suficiente claro que quien firma no pueda después negar su autoría.

6.17.2 Verificación de autenticidad

La confianza digital requiere de verificación, estando la norma a cargo del servidor público de verificar que el archivo firmado utilice un certificado emitido por un ente de certificación acreditado y que las aplicaciones institucionales cuenten a su vez con "mecanismos, reportes o métodos de consulta" que permitan verificar adecuadamente el archivo firmado con una firma electrónica, pues un sistema que acepte un PDF firmado con un certificado revocado o caducado será un fallo grave respecto del control interno (Normas de Control Interno, 2024).

6.17.3 Conservación de archivos electrónicos (Archivo Digital)

Uno de los mayores retos es la conservación a largo plazo, ya que la normativa establece que los documentos firmados tienen que mantenerse en su estado original, garantizando la autenticidad e integridad de los mismos durante un mínimo de siete (7) años (como mínimo, lo que dictan las normas de archivo físico) por lo que las áreas de TI se verán obligadas a crear repositorios digitales seguros con políticas de backup robustas (Norma 410-12), pues la pérdida de un archivo electrónico firmado es equiparable a la pérdida de un documento público físico.

6.17.4 Gestión de certificados digitales y dispositivos (Tokens)

La norma se refiere a la seguridad del medio de firma:

- Dispositivos portables (Tokens): Si la entidad los adquiere, son bienes públicos, y el servidor una vez cesado en funciones tiene que entregar el dispositivo mediante acta de entrega-recepción.
- Informarse sobre la seguridad de claves: Está expresamente prohibido hacer circular las claves de acceso a la firma. El titular es responsable de su correcta utilización.
- Revocación: El servidor tiene la obligación de solicitar la revocación del certificado si tiene sospechas de que su seguridad ha sido vulnerada.

6.17.5 Capacitación específica

De esta manera, la norma clausura el círculo teniendo en cuenta la capacitación específica sobre los "deberes que deben cumplir en el uso de la firma electrónica" dado que muchos de los funcionarios desconocen la existencia de la validez de esta firma electrónica de manera equivalente a una firma manuscrita. La entidad tiene el deber de advertir y en su caso advertir acerca de las consecuencias legales establecidas en dicho uso.

CAPÍTULO VII

7 MARCO METODOLÓGICO DEL CONTROL INTERNO DE TI

El marco metodológico destinado al control interno de Tecnologías de la Información (TI) formula procedimientos y dispositivos a partir de las herramientas y criterios utilizados para valorar, gestionar y además perfeccionar los sistemas tecnológicos de las organizaciones.

7.1 Fundamentos de la Metodología de Evaluación de Normas de Control Interno (NCI) -TI

La evaluación del control interno en el área de las Tecnologías de la información (TI) no es un mero ejercicio de verificación, sino que es un proceso sistemático que intenta determinar el nivel de madurez de la gobernanza en tecnología de la información en las entidades públicas, cuya construcción de la evaluación del Subgrupo 410 de la Contraloría General del Estado (CGE) está en este apartado que establece los fundamentos epistemológicos y técnicos de dicha evaluación.

La metodología propuesta es una metodología que va más allá de la visión del checklist dichotómico (Cumple / No Cumple) al adoptar un enfoque de aseguramiento de la calidad que coincide con el objetivo último de las Normas de Control Interno (NCI)NCI en cuanto promueve la mejora de la gestión pública buscando a la vez garantizar la seguridad razonable del patrimonio estatal.

7.1.1 Enfoque conceptual de la metodología

Está basado en la Teoría de Sistemas y el modelo de Gestión de Riesgos de acuerdo al cual la unidad de TI no se evalúa como una "caja negra", sino como un sistema abierto formado por entradas (recursos, normativas), procesos (desarrollo, operación) y salidas (servicios al ciudadano) inmerso en un entorno de imposibilidad del error.

Este enfoque se apoya en tres pilares conceptuales:

- Prevención vs. detección: La metodología da más peso a la evaluación de los controles de la prevención (diseño de políticas y planificación) que a los de detección. El Acuerdo 004-CG-2023 define que el control interno debe ser ex ante y continuo y no sólo ex Post o después. Por este motivo, la evaluación se centra en existir mecanismos ex ante como la planificación estratégica de TI y la segregación de funciones antes de tener que corregir errores.
- Basado en riesgos: No todas las normas tienen el mismo peso en todos lugares. El enfoque conceptual obliga al auditor a identificar primero los activos críticos. La norma NCI 410-12 (Plan de Contingencias) tiene un peso evaluativo mayor en un hospital público (donde la disponibilidad es vida o muerte) que en una entidad de archivo histórico.
- Seguridad razonable: Esta metodología se apropia de la idea de que el control absoluto es imposible. Se evalúa si los controles llegados a ser implementados generan una "razonable seguridad", entendiendo esta última como la relación costo-beneficio de su implementación.

7.1.2 Integración del proceso administrativo con el ciclo de control interno

La homologación que a continuación se exponen entre las etapas clásicas del Proceso Administrativo (Planificar; Organizar; Dirigir y Controlar) y las normas específicas del Subgrupo 410 a las que se refieren estos mismos autores, que permite al evaluador no tan solo diagnosticar la tecnología, sino la capacidad de gestión administrativa de la unidad, es sin duda uno de los aspectos más importantes aportados por el libro.

En el marco de este libro, se aporta la Tabla 5, que sirve para guiar esta homologación y que es fundamental para construir los papeles de trabajo de la auditoría:

Tabla 5. Matriz de integración: Proceso administrativo vs. NCI-TI.

Fase Administrativa	**Objetivo de Gestión**	**Normas NCI-TI Vinculadas**	**Evidencia de Gestión Esperada**
1. PLANIFICACIÓN	Definir el rumbo estratégico y operativo.	410-04: Plan Estratégico y Operativo 7. 410-09: Planificación de Adquisiciones 8. 410-12: Planificación de Contingencias9.	PETIC aprobado, POA de TI, Estudios de factibilidad y análisis de riesgos.

2. ORGANIZACIÓN	Estructurar recursos y jerarquías.	410-01: Organización de la Unidad 10.	Organigrama funcional, Manual de Descripción de Puestos, Inventario de Activos.
		410-03: Segregación de Funciones 11.	
		410-06: Clasificación de Información12.	
3. DIRECCIÓN	Ejecutar, liderar y tomar decisiones.	410-02: Comité de TI 13.	Actas de Comité de TI, Políticas difundidas, Actas de inicio de proyectos.
		410-05: Políticas y Procedimientos 14.	
		410-07: Administración de Proyectos15.	
4. CONTROL	Medir, corregir y retroalimentar.	410-14: Monitoreo y Evaluación 16.	Informes de indicadores (KPIs), Logs de auditoría, Reportes de vulnerabilidades.

	410-11: Seguridad (Auditoría de Accesos) 17.
	410-10: Control de Infraestructura18.

Fuente: *Elaboración propia.*

Nota. Esta matriz demuestra que el cumplimiento de las NCI-TI cubre integralmente el ciclo de vida de la gestión pública. Una deficiencia en la fase de "Planificación" (ej. falta de PETIC) inevitablemente generará hallazgos en la fase de "Control" (ej. adquisiciones no justificadas).

7.1.3 Relación entre eficacia, eficiencia y calidad

La metodología de evaluación debe distinguir entre tres dimensiones de la situación que a menudo se confunden en la práctica de auditoría. El Acuerdo 004-CG-2023 establece explícitamente que los controles deben garantizar la calidad y la gestión de riesgos.

- Eficacia (cumplimiento de los objetivos y/o resultados esperados): Permite medir el grado en que se alcanzan los resultados esperados; en el caso de NCI-TI, la eficacia se mide verificando si el control implementado realmente mitiga el riesgo.

Ejemplo: La NCI 410-12 exige un Plan de recuperación ante desastres. La eficacia no consiste solamente en tener el documento, sino que, ante la ocurrencia de un incidente, el servicio se restaure en el tiempo que ha sido establecido (RTO).

- Eficiencia (uso de recursos): Se relacionan los resultados con los recursos utilizados. La NCI 410-09 exige análisis costo-beneficio en la adquisición. La metodología permite verificar si la entidad se encuentra gastando excesivamente en controles redundantes o si, por el contrario, se encuentra sub-invirtiendo en áreas críticas.

Ejemplo: Comprar un firewall de última generación (gasto alto), pero no tener personal habilitado para configurar el mismo (NCI 410-16) es una gestión ineficiente.

- Calidad (satisfacción y estándares): Mide las características inherentes del servicio tecnológico. La NCI 410-14 requiere medición de la satisfacción de los clientes internos y externos.

Ejemplo: Un sistema puede ser eficaz (procesa pagos), y eficiente (costo bajo), y aun así posee una mala calidad que conlleva una mala usabilidad o caídas de la aplicación, lo que ni siquiera permita la percepción ciudadana de la calidad (no queremos un sistema que se caiga o sea difícil de usar, independientemente de que sea eficaz o eficiente).

7.1.4 Uso de indicadores, métricas y evidencias

La Objetividad es el principio determinante de esta metodología. De forma que no haya sesgos por parte del evaluador, se establece una jerarquía estricta de medición en función de evidencias. La norma 410-14 manda establecer un marco de trabajo de monitoreo con métricas definidas como se muestra en la Tabla 6.

a) La Pirámide de la evidencia metodológica:

Nivel 1: Evidencia documental (diseño): Hace referencia a que existe normativas en formato físico o digital.

Instrumentos: Políticas firmadas, Manuales de usuario, Contratos con SLA.

Nivel 2: Evidencia de registro (implementación): Hace referencia a pruebas de ejecución del control.

Instrumentos: Bitácoras de operación, Logs de transacciones, Acuerdos de entrega recepción con activos.

Nivel 3: Evidencia analítica (efectividad): Hace referencia al resultado del procesamiento de los datos a efectos de la toma de decisiones.

Instrumentos: Informes de gestión a alta dirección, Resultados de encuestas de satisfacción, Reportes de disponibilidad (Uptime).

Tabla 6. Taxonomía de indicadores para evaluación NCI-TI.

Tipo de Indicador	**Pregunta que responde**	**Ejemplo Normativo**	**Fuente de Datos**
KRI (Riesgo)	¿Qué tan expuestos estamos?	% de servidores sin parches de seguridad (NCI 410-11).	Escáner de Vulnerabilidades.
KPI (Desempeño)	¿Qué tan bien lo hacemos?	Tiempo promedio de resolución de	Sistema de Mesa de Ayuda.

		incidentes (NCI 410-13).	
KCI (Control)	¿Cumplimos la norma?	% de proyectos con acta de cierre formalizada (NCI 410-07).	Portafolio de Proyectos.

Fuente: *Elaboración propia.*

7.1.5 Estructura de evaluación propuesta

Con el objetivo de consolidar los resultados obtenidos en las 17 normas, la metodología del MMCI-TI sugiere la elaboración de un modelo de Madurez de Control Interno de TI (MMCI-TI) para otorgar una calificación a la entidad mediante una escala ordinal que le permita comparar con otras entidades y hacer un seguimiento de las comparaciones históricas.

La escala de esta evolución proviene de la adaptación de aquellos modelos internacionales (CMMI/COBIT) a la realidad normativa ecuatoriana, tal y como queda descrito en el Acuerdo 004-CG-2023 como se evidencia en la Tabla 7.

Tabla 7. Niveles de madurez para la evaluación NCI-TI.

Nivel	**Denominación**	**Descripción Metodológica**	**Estado de Cumplimiento Normativo**
0	INEXISTENTE	Ausencia total de procesos. La tecnología	Incumplimiento sistémico de las NCI. No

		se gestiona de forma caótica.	hay Unidad de TI formal32.
1	INICIAL / AD-HOC	Existen prácticas desorganizadas. El éxito depende de héroes individuales, no de procesos.	Cumplimiento parcial de normas operativas, pero sin políticas formales aprobadas33.
2	REPETIBLE	Los procesos siguen un patrón regular, pero no están documentados formalmente.	Existen procedimientos tácitos ("se hace así siempre"), pero fallan las normas de documentación34.
3	DEFINIDO	Los procesos están documentados, estandarizados y aprobados por la Máxima Autoridad.	Cumplimiento formal de NCI 410-05. Existen manuales y políticas difundidas.
4	ADMINISTRADO	Se mide el cumplimiento mediante indicadores y se controla la calidad.	Cumplimiento de NCI 410-14. Existen reportes de gestión y SLAs monitoreados35.
5	OPTIMIZADO	Mejora continua. Procesos automatizados y eficientes basados en retroalimentación.	Cumplimiento avanzado. Uso de estándares internacionales y auditoría continua.

Fuente: *Elaboración propia.*

7.2 Etapa 1: Alineación institucional para la evaluación

La fase inicial de la metodología no es técnica sino de gobernanza. Para realizar la evaluación del cumplimiento del Subgrupo 410, la entidad debe primero reconocer su realidad operativa respecto a la norma. Tal y como establece el Acuerdo 004-CG-2023, las entidades tienen que "adecuar sus sistemas de control interno", esto es, realizar un proceso formal de diagnóstico antes de cualquier auditoría.

7.2.1 Diagnóstico situacional de TI

La evaluación de la situación es el primer paso. Metodológicamente se plantea utilizar una Lista de Verificación (Checklist) dicotómica fundamentada en los 17 ítems de la Norma 410, que sirve para obtener una "instantánea" rápida sobre el estado de conformidad.

A continuación, en la Tabla 8, se muestra el instrumento propuesto para la recolección de datos en el campo:

Tabla 8. Instrumento de diagnóstico situacional NCI-TI (Ecuador).

Código NCI	**Dominio de Control**	**Pregunta de Verificación (Reactivo)**	**Cumple (Sí/No)**	**Evidencia Preliminar**
410-01	Organización	¿Existe un organigrama aprobado donde conste la Unidad de TI? 4		Estatuto Orgánico.

410-01	Segregación	¿El Oficial de Seguridad de la Información es independiente de la Jefatura de TI? 5	Distributivo de personal.
410-02	Comité TI	¿Se ha constituido formalmente el Comité de TI con la Máxima Autoridad? 6	Actas de conformación.
410-04	Planificación	¿Cuenta la entidad con un Plan Estratégico de TI (PETIC) vigente y aprobado? 7	Documento PETIC físico/digital.
410-04	Presupuesto	¿El presupuesto de TI está desglosado en el POA institucional? 8	Cédula presupuestaria.
410-05	Políticas	¿Existen políticas escritas y difundidas sobre el uso de recursos tecnológicos? 9	Manual de Políticas firmado.
410-07	Proyectos	¿Se utiliza una metodología formal para la administración de proyectos? 10	Guía metodológica de proyectos.

410-08	Software	¿Los desarrollos cuentan con ambientes de pruebas separados de producción? 11	Capturas de pantalla de servidores.
410-09	Adquisiciones	¿Las compras de hardware tienen análisis de costo-beneficio y capacidad? 12	Informes técnicos de compras.
410-10	Inventarios	¿Existe un inventario de activos de TI conciliado con Contabilidad? 13	Reporte de constatación física.
410-11	Seguridad	¿Se han implementado controles alineados a la Ley de Protección de Datos? 14	Matriz de accesos y perfiles.
410-12	Contingencia	¿Existe un Plan de Contingencia y Recuperación de Desastres probado? 15	Acta de simulacro de recuperación.
410-13	Soporte	¿Existe una Mesa de Ayuda que registre incidentes y requerimientos? 16	Reporte de herramienta de tickets.

410-17	Firma Elec.	¿Se utiliza firma electrónica validada en los flujos documentales? 17	Sistema Quipux / Gestión Documental.

Fuente: *Elaboración propia.*

Nota. Un resultado con más del 50% de respuestas negativas indica un nivel de madurez "Inexistente" o "Inicial", lo que alerta sobre un alto riesgo de glosas por parte de la Contraloría (Normas de Control Interno, 2024).

7.2.2 Mapa de riesgos tecnológicos

La normativa 410-12, acompañada del grupo 300, establece la exigencia de administrar los riesgos de la seguridad de la información. Si bien los riesgos cibernéticos (hackers) cuentan con una fuerte presencia en el contexto ecuatoriano, también los riesgos de infraestructura (posibles cortes de energía) y legales son otros factores a considerar evidenciados en la Tabla 9.

Tabla 9. Matriz modelo de riesgos tecnológicos.

ID	Activo	Amenaza (Causa)	Vulnerabilidad (Debilidad)	Impacto (Consecuencia)	NCI Asociada	Nivel Riesgo	Control Propuesto
R-01	Servidor de Base de Datos	Corte de fluido eléctrico (Apagones	UPS con baterías caducadas o generado	Indisponibilidad de servicios al ciudadan	410-12 Plan de Contingencia	ALTO	Mantenimiento preventivo de UPS y

		nacionales).	r sin combustible.	o. Pérdida de datos en tránsito.			generadores (NCI 410-10).
R-02	Información Ciudadana	Ataque de Ransomware.	Falta de parches de seguridad y ausencia de antivirus centralizado.	Secuestro de información, violación a la LOPDP, daño reputacional.	410-11 Seguridad TI	CRÍTICO	Implementación de EDR y política de respaldos inmutables (NCI 410-05).
R-03	Código Fuente (Software)	Salida de personal clave (Programador).	No existe documentación técnica ni repositorio de código.	Imposibilidad de mantener el sistema. "Caja negra".	410-08 Desarrollo	MEDIO	Repositorio Git institucional y documentación obligatoria (NCI 410-08).
R-04	Contrato de Nube	Proveedor declara quiebra.	No existe cláusula de reversibilidad ni backup local.	Pérdida total de la información alojada en el	410-09 Adquisiciones	ALTO	Cláusulas contractuales de salida y backup periódico local

	proveedor .	(NCI 410-09).

Fuente: *Elaboración propia.*

Nota. Esta matriz debe ser validada anualmente por el Comité de TI, conforme a la norma 410-02.

7.3 Etapa 2: Diseño de indicadores para el Subgrupo 410

La norma 410-14 establece que la unidad de TI debe definir "indicadores de rendimiento y métricas". Para hacer que las páginas del libro se llenen de contenido de alto valor, aquí disponemos del Catálogo de Indicadores Estándar que toda entidad pública debería adoptar. Este catálogo convierte la letra de la ley en matemáticas de gestión.

7.3.1 Matriz "estándar – indicador – evidencia"

Esta Tabla10 presentada, es el núcleo metodológico del capítulo, siendo una matriz exhaustiva que correlaciona la norma, la métrica y la evidencia física requerida por un auditor.

Tabla 10. Matriz "estándar – indicador – evidencia".

Norma NCI	**Objetivo del Control**	**Nombre del Indicador**	**Fórmula de Cálculo**	**Frecuencia**	**Evidencia de Auditoría (Soporte)**
410-04 Planificación	Asegurar ejecución del PETIC.	Eficacia del PETIC	$\frac{\text{Proyectos Ejecutados}}{\text{Proyectos Planificados}}$	Semestral	Informes de cierre de proyectos firmados.

410-07 Proyectos	Controlar el cronograma.	Desviación de Cronograma (SPI)	$\frac{\text{Valor Ganado (EV)}}{\text{Valor Planificado (PV)}}$	Mensual	Cronogramas en MS Project / Hojas de control.
410-08 Software	Garantizar calidad del código.	Densidad de Defectos	$\frac{\text{Errores detectados en C}}{\text{Líneas de Código (KLC}}$	Por Liberación	Reportes de SonarQube o herramientas de calidad.
410-09 Adquisiciones	Cumplimiento de Niveles de Servicio.	Cumplimiento de SLA Proveedor	$\frac{\text{Tiempo Servicio Activ}}{\text{Tiempo Total Contrata}} 100$	Mensual	Reportes de disponibilidad del enlace/servicio.
410-10 Mantenimiento	Ejecución del plan preventivo.	Cobertura de Mantenimiento	$\frac{\text{Equipos Mantenidos}}{\text{Total Equipos Inventar}} 100$	Trimestral	Actas de mantenimiento preventivo firmadas.
410-11 Seguridad	Gestión de vulnerabilidades.	Tasa de Parcheo	$\frac{\text{Servidores con Parches}}{\text{Total Servidores Crí}} 100$	Mensual	Reportes de escaneo de vulnerabilidades (Nessus/OpenVAS).

410-12 Contingencia	Preparación ante desastres.	Eficacia de Simulacros	$\frac{\text{Simulacros Exitosos}}{\text{Simulacros Ejecutados}}$	Anual	Actas de evaluación del simulacro de DRP.
410-13 Soporte	Eficiencia en atención al usuario.	Resolución en Primer Nivel	$\frac{\text{Tickets resueltos por}}{\text{Total Tickets Recil}} 100$	Mensual	Estadísticas del sistema de Mesa de Ayuda.
410-13 Soporte	Satisfacción del usuario.	Índice de Satisfacción (CSAT)	Promedio de encuestas (Escala 1-5).	Trimestral	Encuestas digitales post-atención.
410-16 Capacitación	Ejecución del plan de formación.	Cobertura de Capacitación	$\frac{\text{Funcionarios Capacita}}{\text{Total Personal Objeti}} 100$	Anual	Certificados de asistencia y aprobación.

Fuente: *Elaboración propia.*

7.3.2 Validación técnica de indicadores

Para dar robustez académica, se explica que cada indicador de la tabla anterior debe pasar por un filtro de validación. Según (Kaplan & Norton, 1992), los indicadores deben ser SMART.

- S (Específico): El indicador "Mejorar la seguridad" es inválido. El correcto es "Reducir incidentes de virus en un 10%".

- M (Medible): Debe existir una fuente de datos (Logs, Base de datos). Si no hay datos, el indicador es una opinión.
- A (Alcanzable): Metas realistas bajo el presupuesto actual.
- R (Relevante): Debe importar a la misión institucional (Norma 410-14).
- T (Temporal): Debe tener un periodo definido (mensual, anual).

7.3.3 Diseño de tableros de control

La norma 410-14 establece la obligación de presentar informes a la Alta Dirección. Por ello es fundamental ilustrar cómo se ve en la Figura 1.

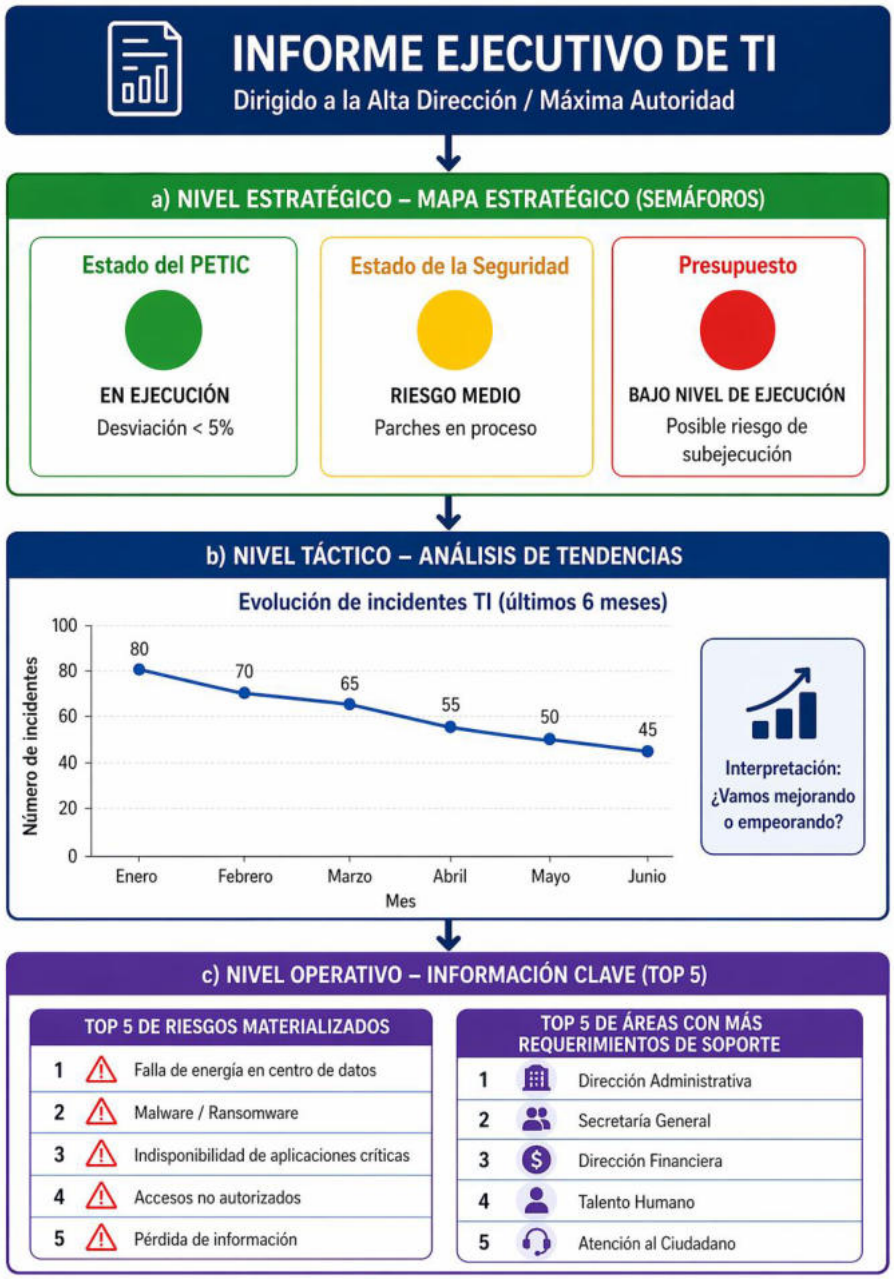

Figura 1. Estructura de un informe ejecutivo de TI según NCI.

Fuente: *Generado con inteligencia artificial IA.*

La Figura 1, muestra una Descripción detallada para el lector, siendo que, un informe de control interno para el Contralor o la Máxima Autoridad no debe tener código técnico, sino que debe estructurarse en tres niveles:

a) Mapa estratégico (semáforos)

- Estado del PETIC: 🟢 (En ejecución, desviación < 5%).
- Estado de la Seguridad: 🟡 (Riesgo medio, parches en proceso).
- Presupuesto: 🔴 (Bajo nivel de ejecución, posible riesgo de subejecución).

b) Nivel Táctico (tendencias)

Gráfico de líneas mostrando la evolución de incidentes en los últimos 6 meses. ¿Vamos mejorando o empeorando?

c) Nivel operativo (Top 5)

- Top 5 de riesgos materializados.

Top 5 de áreas con más requerimientos de soporte.

CONCLUSIONES

Los contenidos que se desarrollan en este libro muestran que la Gestión de las Tecnologías de la Información en el sector público forma parte de una política estratégica para el funcionamiento institucional. Una buena planificación de los procesos tecnológicos, la asignación de las tareas y la incorporación de las TI en la planificación institucional es un buen recurso para aumentar la eficacia operativa pública y, al mismo tiempo, llevar a cabo un acentuado refuerzo en la calidad del servicio público. Desde ese punto de vista, la administración de TI requiere una visión estructurada de acuerdo con lo que son las bases del sistema que requiere tanto la visión técnica como la administrativa que condiciona su acción.

El análisis del control interno y de su aplicación en el terreno del tipo tecnológico muestra que el control interno es una buena vía para prevenir riesgos, homogeneizar procesos y asegurar el cumplimiento de la normativa vigente. El análisis realizado del Subgrupo 410 hace entender el mismo como un marco orientado a poder evaluar la madurez en los procesos tecnológicos y una base de apoyo a fin de emergente de los sistemas de control interno a la gobernanza institucional. Su aceptación contribuye a establecer mecanismos de control más fuertes y promueve la transparencia en la toma de decisiones de los recursos informáticos.

La constitución metodológica presentada en este artículo propone un marco práctico para evaluar el nivel de funcionamiento de la gestión tecnológica de las instituciones públicas. La misma permite obtener diagnósticos fiables para la determinación de acciones de mejora y la

posibilidad de despertar una cultura orientada a la eficiencia y al uso responsable de los recursos tecnológicos. En gran medida, las conclusiones extraídas reflejan que sólo será posible el fomentar la gestión de TI en aquellas instituciones que sean capaces de aplicar estándares y consolidar procedimientos, así como de establecer sistemas de control interno que aseguren, precisamente, la seguridad y continuidad, además de los niveles de calidad de los servicios que se ofrecen a sus ciudadanos.

GLOSARIO

Acceso remoto: Proceso que permite a usuarios conectarse a sistemas institucionales desde ubicaciones externas. Requiere controles de seguridad para evitar intrusiones y garantizar confidencialidad.

Activo tecnológico: Recurso informático que aporta valor a la institución, como hardware, software, datos o infraestructura. Su gestión adecuada asegura continuidad operativa y protección de la información.

Administración pública: Conjunto de entidades y procesos que gestionan recursos estatales para satisfacer necesidades ciudadanas. Se rige por principios de eficiencia, transparencia y responsabilidad.

Alta disponibilidad: Capacidad de un sistema para permanecer operativo la mayor parte del tiempo, reduciendo interrupciones. Se logra mediante redundancia, monitoreo y planes de continuidad.

Análisis de brechas: Proceso que compara la situación actual con un estándar deseado. Permite identificar deficiencias y orientar acciones de mejora en la gestión de TI.

Arquitectura empresarial: Modelo que integra procesos, datos, tecnología y estrategia. Facilita alineación institucional.

Arquitectura de TI: Estructura que organiza componentes tecnológicos para soportar operaciones. Permite estandarización.

Auditoría informática: Evaluación técnica y sistemática de procesos, controles y sistemas tecnológicos. Busca verificar cumplimiento normativo y detectar riesgos o ineficiencias.

Autenticación: Mecanismo que valida la identidad de un usuario o dispositivo antes de permitir acceso. Contribuye a la seguridad y protección de sistemas y datos.

Automatización: Uso de software para ejecutar procesos sin intervención humana. Incrementa eficiencia y reduce errores.

Backup (respaldo): Copia de seguridad que permite recuperar datos ante fallos, ataques o pérdidas. Es esencial para la continuidad operativa institucional.

Benchmarking: Comparación de prácticas institucionales con estándares o referentes del sector. Facilita el mejoramiento continuo en la gestión tecnológica.

Big Data: Conjunto de datos masivos procesados con tecnologías avanzadas. Permite análisis profundo para decisiones.

Brecha digital: Diferencia existente en el acceso, uso y aprovechamiento de tecnologías entre grupos o instituciones. Afecta eficiencia y calidad de servicios públicos.

Capacitación tecnológica: Proceso de formación del talento humano en temas de TI. Aumenta competencias y desempeño.

Capa de red: Nivel técnico encargado de interconectar dispositivos. Soporta comunicación institucional.

Certificación digital: Documento electrónico que valida identidades. Se usa en firmas y trámites seguros.

Ciclo de vida del sistema: Etapas desde la planificación hasta el retiro de un sistema informático. Su adecuada gestión garantiza eficiencia y sostenibilidad tecnológica.

Ciberseguridad: Conjunto de prácticas para proteger sistemas y datos ante ataques o accesos no autorizados. Reduce riesgos operativos y reputacionales.

Ciberataque: Acción que busca vulnerar sistemas para causar daño, robar información o interrumpir servicios. Requiere respuestas rápidas y medidas preventivas.

Cloud computing: Modelo de servicios que permite acceso remoto a infraestructura, plataformas o software. Reduce costos y facilita escalabilidad institucional.

COBIT: Marco internacional de gobernanza de TI que establece principios, procesos y controles. Orienta la alineación tecnológica con los objetivos institucionales.

Código de Normas de Control Interno (COCOI): Normativa ecuatoriana que regula prácticas de control interno. El Subgrupo 410 establece lineamientos específicos para la gestión de TI.

Comité de TI: Órgano interno encargado de coordinar decisiones tecnológicas. Garantiza gobernanza, priorización y coherencia operativa.

Compliance: Cumplimiento normativo en materia tecnológica y administrativa. Evita sanciones y asegura alineación con regulaciones vigentes.

Controles compensatorios: Medidas alternativas usadas cuando un control principal no puede implementarse. Reducen riesgos y fortalecen la seguridad institucional.

Control interno: Conjunto de políticas y procedimientos orientados a asegurar eficiencia, legalidad y confiabilidad de la información institucional.

Continuidad operativa: Capacidad de una entidad para mantener funciones críticas ante interrupciones. Requiere planificación, redundancia y respuesta ante incidentes.

Control de acceso: Mecanismos que regulan quién puede ingresar a sistemas o datos. Previenen intrusiones.

Datos abiertos: Información institucional publicada para acceso público. Promueve transparencia y participación ciudadana.

Desempeño tecnológico: Medición de la eficiencia operativa de sistemas y servicios de TI. Facilita la toma de decisiones sobre mejoras.

Diagnóstico tecnológico: Evaluación integral de infraestructura, procesos y controles. Permite definir prioridades de inversión y mejora.

Disponibilidad: Condición que asegura acceso oportuno a los sistemas. Es un pilar de la seguridad de la información.

Encriptación: Proceso que transforma datos para protegerlos ante accesos no autorizados. Es clave para la seguridad en tránsito y almacenamiento.

Estrategia digital: Plan institucional para orientar el uso de tecnologías hacia objetivos organizacionales. Impulsa modernización y eficiencia.

Evaluación de riesgos: Identificación y análisis de amenazas que podrían afectar procesos de TI. Permite priorizar controles y mitigaciones.

Firewall: Sistema de protección que controla el tráfico entre redes. Evita accesos no autorizados y ataques.

Gestión de incidentes: Proceso para identificar, registrar y solucionar problemas tecnológicos. Minimiza impactos operativos.

Gestión de infraestructura: Administración de hardware, redes y equipos institucionales. Asegura disponibilidad y desempeño óptimo.

Gestión de riesgos TIC: Conjunto de actividades para prevenir daños en sistemas, datos y servicios. Reduce vulnerabilidades.

Gestión documental: Proceso para organizar, almacenar y proteger información institucional. Facilita transparencia y control.

Gestión del cambio: Proceso que guía la adopción de nuevas tecnologías. Reduce resistencia y fallas de implementación.

Gestión del conocimiento: Prácticas para capturar y compartir información institucional. Mejora procesos y decisiones.

Gobierno digital: Modelo estatal que integra tecnologías para optimizar servicios públicos. Busca simplificación y eficiencia.

Gobernanza de TI: Estructura que orienta decisiones tecnológicas hacia objetivos institucionales. Requiere liderazgo, procesos y control.

Hardware: Componentes físicos de un sistema informático. Su mantenimiento y actualización influyen en el rendimiento institucional.

Identidad digital: Conjunto de atributos electrónicos que identifican a una persona. Es vital para autenticación y servicios en línea.

Incidente de seguridad: Evento que compromete la confidencialidad, integridad o disponibilidad. Requiere análisis y acciones correctivas.

Indicadores de gestión: Métricas que permiten medir resultados en TI. Facilitan supervisión y mejora continua.

Infraestructura crítica: Equipos y sistemas esenciales para la operación institucional. Su falla afecta servicios clave.

Integridad del dato: Principio que garantiza que la información no sea modificada de forma no autorizada. Es indispensable en procesos críticos.

Interoperabilidad: Capacidad de sistemas para intercambiar información de forma segura y eficiente. Es clave para la modernización estatal.

Integración de sistemas: Proceso que permite que aplicaciones distintas interactúen. Mejora eficiencia y reduce duplicidades.

Inventario de activos: Registro actualizado de recursos tecnológicos institucionales. Permite control y seguimiento eficiente.

ISO 27001: Estándar internacional de gestión de seguridad de la información. Define controles para proteger datos y sistemas.

ISO 20000: Norma enfocada en la gestión de servicios de TI. Promueve calidad, orden y eficiencia operativa.

ITIL: Marco de mejores prácticas para la gestión de servicios tecnológicos. Establece procesos estandarizados y orientados al usuario.

Jefe de TI: Responsable de coordinar la función tecnológica. Administra recursos, procesos y servicios informáticos.

Licenciamiento de software: Cumplimiento legal respecto al uso de programas informáticos. Evita riesgos legales y financieros.

Log de auditoría: Registro automático de actividades en sistemas. Permite trazabilidad y monitoreo.

Manual de procedimientos: Documento que define pasos, responsabilidades y controles. Facilita uniformidad y supervisión.

Marco normativo: Conjunto de leyes, estándares y regulaciones que rigen la gestión tecnológica institucional.

Matriz de riesgos: Herramienta que clasifica amenazas según probabilidad e impacto. Orienta la priorización de controles.

Mecanismos de control: Acciones que previenen errores y riesgos en procesos tecnológicos. Son pilares del control interno.

Metadata: Datos que describen otros datos. Facilitan búsqueda, clasificación y gobernanza de información.

Migración de sistemas: Proceso de mover aplicaciones o datos a nuevas plataformas. Requiere planificación y pruebas.

Monitoreo tecnológico: Supervisión continua del desempeño de sistemas. Detecta fallas y previene interrupciones.

Nivel de madurez: Grado en que un proceso tecnológico está estandarizado y optimizado. Permite evaluar evolución institucional.

Nivel de servicio (SLA): Acuerdo que define tiempos, calidad y disponibilidad esperada en servicios tecnológicos.

Plataforma tecnológica: Conjunto integrado de sistemas y herramientas que soportan procesos institucionales.

Política de seguridad: Directrices que regulan el comportamiento tecnológico. Buscan proteger activos y servicios.

Privacidad de datos: Derecho a que la información personal sea protegida y tratada adecuadamente.

Procesos críticos: Actividades cuyo funcionamiento es esencial para la institución. Requieren controles estrictos.

Programa de mejora: Plan que define acciones para optimizar procesos tecnológicos. Se basa en diagnósticos previos.

Protocolo de comunicación: Reglas que permiten el intercambio de datos entre sistemas. Aseguran compatibilidad.

Red institucional: Conjunto de dispositivos interconectados para compartir información y servicios.

Rendición de cuentas: Obligación institucional de informar y justificar decisiones. Se fortalece mediante TI confiables.

Riesgo tecnológico: Amenaza que puede afectar sistemas o servicios informáticos. Debe ser gestionado y mitigado.

Seguridad lógica: Controles orientados a proteger software y datos. Complementa la seguridad física.

Seguridad física: Protección de infraestructura ante daños, robos o accesos no autorizados.

Servidor: Equipo que almacena y administra servicios, aplicaciones o datos institucionales.

Sistema de información: Conjunto de componentes que gestionan datos para apoyar procesos institucionales.

Sistema crítico: Aplicación cuyo fallo afecta funciones esenciales. Requiere redundancia y monitoreo constante.

Sistema legado: Sistema antiguo aún en uso. Representa riesgos de compatibilidad y soporte.

Software: Programas que permiten operar equipos y sistemas. Su gestión influye en eficiencia.

Subgrupo 410: Normativa de control interno que regula la función de TI en Ecuador. Establece obligaciones y controles clave.

Trazabilidad: Capacidad de rastrear acciones o cambios dentro de un sistema. Es fundamental en auditoría.

Transformación digital: Proceso de modernización institucional mediante tecnologías. Busca eficiencia y servicios innovadores.

Usuario final: Persona que utiliza sistemas o servicios tecnológicos. Sus necesidades deben ser consideradas en la gestión.

Valor público: Beneficio generado para la sociedad a partir de procesos institucionales. Las TI contribuyen decisivamente a su creación.

Virtualización: Tecnología que permite crear versiones lógicas de recursos físicos. Optimiza almacenamiento y servidores.

Vulnerabilidad: Debilidad que puede ser explotada por amenazas. Debe ser identificada y corregida.

BIBLIOGRAFÍA

Amend, J., Fridgen, G., Rieger, A., Roth, T., & Stohr, A. (2021). The Evolution of an Architectural Paradigm - Using Blockchain to Build a Cross-Organizational Enterprise Service Bus. *Proceedings of the Annual Hawaii International Conference on System Sciences*, *2020-January*, 1–10. https://doi.org/10.24251/HICSS.2021.522

Angraini, Alias, R. A., & Okfalisa. (2019). Information Security Policy Compliance: Systematic Literature Review. *Procedia Computer Science*, *161*, 1216–1224. https://doi.org/10.1016/J.PROCS.2019.11.235

Arroyo, F. R. M., & Miguel, L. J. (2020). The Role of Renewable Energies for the Sustainable Energy Governance and Environmental Policies for the Mitigation of Climate Change in Ecuador. *Energies*, *13*(15). https://doi.org/10.3390/EN13153883

Cadena, N. (2023). NORMAS DE CONTROL INTERNO DE TECNOLOGÍAS DE LA INFORMACIÓN - CGE. *AUDITORÍA DE SISTEMAS INFORMÁTICOS*.

Cedergren, A., & Hassel, H. (2025). Business Continuity Management in Public Sector Organizations: Development, Challenges, and Ways Forward. *Journal of Contingencies and Crisis Management*, *33*(2), e70055. https://doi.org/10.1111/1468-5973.70055;PAGE:STRING:ARTICLE/CHAPTER

Cevallos, S. (2023). The Role of Locality in Public Service Management of Ecuador. *Academic and Applied Research in Military and Public Management Science*, *22*(1), 51–60. https://doi.org/10.32565/AARMS.2023.1.4

CONSTITUCION DE LA REPUBLICA DEL ECUADOR. (2011). CONSTITUCION DE LA REPUBLICA DEL ECUADOR 2008 Decreto Legislativo 0 Registro Oficial. *Decreto Legislativo 0*. www.lexis.com.ec

Criado, J. I., & Garcia, J. R. (2019). Creating public value through smart technologies and strategiesFrom digital services to artificial intelligence and beyond. *International Journal of Public Sector Management*, *32*(5), 438–450. https://doi.org/10.1108/IJPSM-07-2019-0178

Flores, P. R., Lopez, C. R., Flores, P. R., & Lopez, C. R. (2025a). Gobernanza de las tecnologías de la información en el desarrollo corporativo. *Revista InveCom*, *5*(1). https://doi.org/10.5281/ZENODO.11374432

Flores, P. R., Lopez, C. R., Flores, P. R., & Lopez, C. R. (2025b). Gobernanza de las tecnologías de la información en el desarrollo corporativo. *Revista InveCom*, *5*(1). https://doi.org/10.5281/ZENODO.11374432

Fonseca, L., Cardoso, M. C., Pereira, M. T., & Ávila, P. (2021). ISO 9001 Certification Benefits: A Principal Component Analysis.

FME Transactions, *49*(4), 835–841. https://doi.org/10.5937/FME2104835F

Gavilanes, A., & Merchán, V. (2022). Information technology governance: an analysis of the approach in Ecuador. *Bulletin of Electrical Engineering and Informatics*, *11*(1), 466–476. https://doi.org/10.11591/EEI.V11I1.3449

Iddrisu, I., & Fuseini, I. (2025). The impact of digital technologies on public service delivery: the role of organizational structures and decision-making. *International Journal of Organizational Analysis*. https://doi.org/10.1108/IJOA-10-2024-4918

Imran, N. (2025). Implementation of Positive Train Control (PTC) or ETC (European Train Control System) in Bangladesh Railways: A Sustainable Approach. *American Journal of Traffic and Transportation Engineering*, *10*(4), 90–95. https://doi.org/10.11648/J.AJTTE.20251004.12

ISACA. (2019). *COBIT 2019 Framework Introduction and Methodology Res Spa 0519 | PDF | Cobit | Business*. CQBIT. https://es.scribd.com/document/839065057/COBIT-2019-Framework-Introduction-and-Methodology-Res-Spa-0519-Convertido

Kaplan, R., & Norton, D. (1992). *The Balanced Scorecard—Measures that Drive Performance*. https://hbr.org/1992/01/the-balanced-scorecard-measures-that-drive-performance-2

Khan, M. N. I. (2025). CROSS-BORDER DATA PRIVACY AND LEGAL SUPPORT: A SYSTEMATIC REVIEW OF INTERNATIONAL COMPLIANCE STANDARDS AND CYBER LAW PRACTICES. *American Journal of Scholarly Research and Innovation*, *04*(01), 138–174. https://doi.org/10.63125/A4GBEB22

Krotova, E. L., Subbotina, Yu. V., Ermakov, D. G., & Tishin, K. L. (2024). PECULIARITIES OF DEVELOPMENT AND IMPLEMENTATION OF THE ELECTRONIC VOTING SYSTEM. *Journal of the Ural Federal District. Information Security*, *24*(1). https://doi.org/10.14529/SECUR240102

Landsittel, D. L., Landes, C., Hollein, M. N., & Chambers, R. F. (2013). *COSO 2013 - Marco y Apéndices PDF | PDF*. https://es.scribd.com/document/433573419/COSO-2013-Marco-y-Apendices-pdf

LEY ORGÁNICA DE PROTECCIÓN, & DE DATOS PERSONALES. (2021). *Quinto Suplemento*. Quinto Suplemento. https://www.telecomunicaciones.gob.ec/wp-content/uploads/2021/06/Ley-Organica-de-Datos-Personales.pdf

LEY ORGÁNICA PARA LA TRANSFORMACIÓN DIGITAL Y AUDIOVISUAL. (2023). *LEY ORGÁNICA PARA LA TRANSFORMACIÓN DIGITAL Y AUDIOVISUAL*. LEXIS. https://nmslaw.com.ec/blog/2023/02/12/ley-transformacion-digital/

Liu, Z. Y., Lomovtseva, N., & Korobeynikova, E. (2020). Online Learning Platforms: Reconstructing Modern Higher Education. *Int. J. Emerg. Technol. Learn.*, *15*(13), 4–21. https://doi.org/10.3991/IJET.V15I13.14645

Macias, V., Suárez, A., Gutiérrez, R., & Saavedra, C. (2025). Política Pública para la Transformación Digital del Ecuador © Ministerio de Telecomunicaciones y Sociedad de la Información. *Ministerio de Telecomunicaciones y de La Sociedad de La Información*. https://www.gobiernoelectronico.gob.ec/wp-content/uploads/2025/03/INSTRUMENTO-Politica-Publica-para-la-Transformacion-Digital-Ecuador-2025-2030-MINTEL-signed_f.pdf?utm_source=chatgpt.com

MacLean, D., & Titah, R. (2023). Implementation and impacts of IT Service Management in the IT function. *International Journal of Information Management*, *70*, 102628. https://doi.org/10.1016/J.IJINFOMGT.2023.102628

Martínez, X. B. (2022). Posmodernidad, gestión pública y tecnologías de la información y comunicación en la Administración pública de Ecuador. *Estado & Comunes*, *1*(14), 113–131. https://doi.org/10.37228/estado_comunes.v1.n14.2022.244

Mera, C., Vera, D., Mendoza, J. L., Briones, J. A., & Mendoza, H. F. (2021). GESTIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN EN INSTITUCIONES PÚBLICAS. In *GESTIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN EN INSTITUCIONES PÚBLICAS* (2021st ed., Vol. 1). scuela Internacional de Negocios

y Desarrollo Empresarial de Colombia. https://doi.org/10.34893/TNG4-8488

Merchán, V., & Zambrano, D. (2023). Budget and capabilities of information technology governance: empirical analysis in higher education institutes. *Bulletin of Electrical Engineering and Informatics*, *12*(2), 1137–1147. https://doi.org/10.11591/EEI.V12I2.4302

Mergel, I. (2016). Agile innovation management in government: A research agenda. *Government Information Quarterly*, *33*(3), 516–523. https://doi.org/10.1016/J.GIQ.2016.07.004

Mergel, I. (2019). Digital service teams in government. *Gov. Inf. Q.*, *36*(4). https://doi.org/10.1016/J.GIQ.2019.07.001

Merino, J. A. V., & Chávez, W. E. Z. (2020). La gestión del presupuesto por resultados y la calidad del gasto en gobiernos locales. *Revista Científica Visión de Futuro*, *24*(2). https://visiondefuturo.fce.unam.edu.ar/index.php/visiondefuturo/article/view/442

Mina, S. D., Hernández, M. D., Carriel, L. D., & Zamora, D. J. (2025). Gobierno Electrónico en Ecuador para la agilización de trámites en línea mejorando el servicio público. *Innova Science Journal*, *3*(3), 622–634. https://doi.org/10.63618/OMD/ISJ/V3/N3/106

Mullo, X., & Camero, R. (2025). Políticas de seguridad de la información según la norma iso 27001 para el municipio de

Guaranda, Bolívar, Ecuador. *593 Digital Publisher CEIT*, *10*(3), 340–351. https://doi.org/10.33386/593DP.2025.3.3134

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

Norma Jurídica Oficial. (2020). Tipo de la Norma. *Ley Orgánica de Transparencia y Acceso a La Información Pública - LOTAIP*. https://www.azuay.gob.ec/wp-content/uploads/2020/06/Literal_a2-Base_legal_que_rige_a_la_institucion-JAP-3.pdf

Normas de Control Interno. (2024). *CONTRALORIA GENERAL DEL ESTADO :: Normas de Control Interno*. Normas de Control Interno. https://www.contraloria.gob.ec/Portal/Sistema/NormasControlnterno

Núñez, M., & Pérez, C. (2022). New challenges in higher education: A study of the digital competence of educators in Covid times. *Technological Forecasting and Social Change*, *174*. https://doi.org/10.1016/J.TECHFORE.2021.121270

Paguay, C., Cevallos, D., Rodríguez, A., & Estrada, J. (2025). Transparency Unleashed: Privacy Risks in the Age of E-Government. *Informatics*, *12*(2). https://doi.org/10.3390/INFORMATICS12020039

Peña, U. (2023). *Contraloria General Del Estado Manual | PDF | Auditoría | Planificación*. Manual General de Auditoría Gubernamental de La Contraloría General Del Estado de Ecuador. https://es.scribd.com/document/474922720/contraloria-general-del-estado-manual

Peñaherrera, W. P., Peñaherrera, S. J., & Espinoza, P. S. (2021). Covid-19: La transformación de la educación en el Ecuador mediante la inclusión de herramientas tecnológicas en las clases virtuales. *Dominio de Las Ciencias*, *7*(1), 898–908. https://doi.org/10.23857/dc.v7i1.1684

Prates, J. C. R., Gomes, W. P., Pinheiro, L. E. T., & Avelino, B. C. (2023). Reacción de la bolsa brasileña a las notas explicativas del COVID-19 en los estados financieros del sector agropesquero de B3. *Contabilidad y Negocios*, *18*(35), 39–66. https://doi.org/10.18800/CONTABILIDAD.202301.008

Quiñónez, M. del P., Jacho, B., & Moran, B. (2024). LA IMPORTANCIA DE LA AUDITORÍA INTERNA EN LA GESTIÓN DE RIESGOS EMPRESARIALES. *Ciencia y Desarrollo*, *27*(1), 77. https://doi.org/10.21503/CYD.V27I1.2544

Reis, J., Amorim, M., Melão, N., Cohen, Y., & Rodrigues, M. (2020). Digitalization: A Literature Review and Research Agenda. *Lecture Notes on Multidisciplinary Industrial Engineering*, *Part F201*, 443–456. https://doi.org/10.1007/978-3-030-43616-2_47

Salazar, F. O. L., Oleas, J. P. P., Tacuri, A. I. A., Naranjo, T. Y. C., & Vega, F. M. S. (2025). Transformación Digital del Sector Turístico en Ecuador: Retos Administrativos y Marco Legal. *Ibero Ciencias - Revista Científica y Académica - ISSN 3072-7197*, *4*(3), 527–541. https://doi.org/10.63371/IC.V4.N3.A135

Salazar, Torres, M., Rodríguez, M., & Feijoo, E. (2020). FISCALÍA GENERAL DEL ESTADO COMITÉ EDITORIAL. *FISCALIA GENERAL DEL ESTADO*. https://www.fiscalia.gob.ec/pdf/politica-criminal/revista-Perfil-Criminologico-julio-2020.pdf

Silva, R., Medina, J., Alvarado, R., Recalde, T., Noboa, C., Martillo, I., & Alvarez, P. (2017). Interoperable Electronic Health Records (EHRs) for Ecuador. *Journal of Health and Medical Informatics*, *8*(03), 1–7. https://doi.org/10.4172/2157-7420.1000271

Siponen, M., Adam Mahmood, M., & Pahnila, S. (2014). Employees' adherence to information security policies: An exploratory field study. *Information & Management*, *51*(2), 217–224. https://doi.org/10.1016/J.IM.2013.08.006

Sofyani, H., Riyadh, H. A., & Fahlevi, H. (2020). Improving service quality, accountability and transparency of local government: The intervening role of information technology governance. *Cogent Business & Management*, *7*(1). https://doi.org/10.1080/23311975.2020.1735690

Soledispa, B. I., & Rodríguez, K. I. (2021). El control interno y su incidencia en la gestión administrativa del GAD Pedro Carbo, Ecuador. *Dominio de Las Ciencias, ISSN-e 2477-8818, Vol. 7, No. 6, 2021 (Ejemplar Dedicado a: OCTUBRE 2021), Págs. 162-179*, *7*(6), 162–179. https://doi.org/10.23857/dc.v7i4.2221

Toapanta, S. M. T., Ochoa, I. N. C., Sanchez, R. A. N., & Mafla, L. E. G. (2019). Impact on Administrative Processes by Cyberattacks in a Public Organization of Ecuador. *2019 Third World Conference on Smart Trends in Systems Security and Sustainablity (WorldS4)*, 270–274. https://doi.org/10.1109/WORLDS4.2019.8903967

Twizeyimana, J. D. (2019). The public value of E-Government – A literature review. *Government Information Quarterly*, *36*(2), 167–178. https://doi.org/10.1016/J.GIQ.2019.01.001

Vallejo, C. (2022). El sistema de control interno y la gestión pública: Una revisión sistemática. *Ciencia Latina Revista Científica Multidisciplinar*, *6*(2), 2316–2335. https://doi.org/10.37811/CL_RCM.V6I2.2030

Valverde, F., & Llorens, F. (2016). Proposal of a Framework of IT Governance for Public Universities in Ecuador. *ACM International Conference Proceeding Series*, *02-04-Nove*, 1209–1216. https://doi.org/10.1145/3012430.3012671;CSUBTYPE:STRING:CONFERENCE

Vasconez, J., Alexander, H., & Ortiz, E. (2025). Digital Health Transformation in Ecuador: Progress, Barriers, and Future

Directions. *Journal of Medical Systems*, *49 1*(1). https://doi.org/10.1007/S10916-025-02174-3

Vial, G. (2019). Understanding digital transformation: A review and a research agenda. *Journal of Strategic Information Systems*, *28*(2), 118–144. https://doi.org/10.1016/J.JSIS.2019.01.003

Villao, D., Vera, G., Duque, V., & Mazón, L. (2023). Opportunities and Challenges of Digital Transformation in the Public Sector: The Case of Ecuador. *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, *14108 LNCS*, 3–15. https://doi.org/10.1007/978-3-031-37117-2_1

Weill, Peter., & Ross, J. W. . (2004). IT governance : how top performers manage IT decision rights for superior results. *Editorial: Harvard Business School Press*, 269.

Zaitouni, M., Hewapathirana, G., Mostafa, M., Al Hajj, R., & ElMelegy, A. R. (2024). Work-life balance: A landscape mapping of two decades of scholarly research. *Heliyon*, *10*(14), e34084. https://doi.org/10.1016/J.HELIYON.2024.E34084

Tomo I Gestión de tecnologías de la información: una perspectiva del control interno en el sector público, se publicó en el mes de diciembre de 2025.

ISBN: 978-9907-0-0579-0

Grupo Editorial BLR
Ecuador
Cel: +593 98 320 4362
https://grupoblr.com/
publicaciones@grupoblr.com

BIOGRAFÍA DE LOS AUTORES

Byron Napoleón Cadena Oleas:
Profesor investigador de la Escuela Superior Politécnica de Chimborazo, Ingeniero de Empresas, Técnico en Programación de Sistemas; Doctor en Ciencias Económicas, Magister en Informática Aplicada, Magister en Auditoria Integral, Especialista en Gestión Pública, Diploma Superior en Proyectos y Transferencia de Tecnologías. Profesor Titular en la Escuela Superior Politécnica de Chimborazo en los noveles de Grado y Posgrado. Coordinador Académico de la Carrera de Ingeniería de Empresas – Modalidad Dual en la ESPOCH. Desempeñó varios cargos en el ámbito público, como privado, entre ellos: Alcalde del Cantón Riobamba. Concejal Cantón Riobamba. Tesorero Municipal. Presidente de Empresas Públicas. Presidente del Consejo Cantonal de Planificación de Riobamba. Consejero Provincial en el Gobierno Autónomo Descentralizado Provincial de Chimborazo. Presidente del Consejo Cantonal de Protección de Derechos.

Raquel Virginia Colcha Ortiz:
Docente Investigadora de la Escuela Politécnica Superior de Chimborazo, Doctora en Gestión Pública y Gobernabilidad, Magíster en Contabilidad y Auditoría con mención en Gestión Tributaria, Magíster en Gestión Empresarial, Licenciada en Contabilidad Superior, Auditoría y Finanzas (CPA). Docente de pregrado y posgrado en varias Universidades Ecuatorianas. Presidenta del Consejo de Profesores y Pedagogos encargados de preparar el examen de selección del Contralor General de la Nación, Reconocimiento como Investigadora Principal, Premio Saber Ser y Ser a la Investigación Científica Nacional e Internacional, Profesional Contable Destacada, Directora y Subdirectora de Proyectos de Investigación y Vinculación con la Sociedad.

Wilmer Enrique Mera Herrera:
Investigador, Doctorante en Dirección de Proyectos Magister en Gestión Empresarial, Magister en Matemática Aplicada con mención en Matemática Computacional, Ingeniero Industrial, Tecnólogo en Aviónica, Coordinador de

Posgrado UNACH, Investigador en proyectos de Investigación UNACH, publicaciones científicas, asesor de tesis de posgrado.

Michael Adrián Erazo Granizo:

Ingeniero en Informática e ingeniero en Contabilidad y Auditoría (CPA), con formación de posgrado en Matemática Aplicada mención en Matemática Computacional, y un MBA. Me desempeño como técnico de apoyo a la investigación en la UNACH (Ecuador), con experiencia en docencia universitaria, investigación y gestión académica, complementada por asesoría contable y administrativa y énfasis en análisis cuantitativo y modelación matemática.

TOMO I GESTIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN: UNA PERSPECTIVA DEL CONTROL INTERNO EN EL SECTOR PÚBLICO

Estimado lector, este libro constituye una guía integral sobre la gestión y el control de las tecnologías de la información en el sector público de Ecuador, vinculando la administración operativa con las normas de la Contraloría General del Estado.

El documento detalla el cumplimiento del Subgrupo 410, que abarca desde la planificación estratégica y la seguridad de la información hasta la gestión de proyectos y la continuidad de servicios.

Mediante una metodología basada en niveles de madurez y gestión de riesgos, la obra busca que las instituciones estatales dejen atrás los procesos manuales y adopten un modelo de transformación digital que asegure la eficiencia, la transparencia y la protección de los activos de información institucionales.

Agradecemos a todos los lectores que se acercan a esta obra con ánimo de aprender, aplicar y transformar.

Grupo Editorial BLR
Ecuador
Cel: +593 98 320 4362
https://grupoblr.com/
publicaciones@grupoblr.com

GRUPO BLR

ISBN: 978-9907-0-0579-0