SUPLEMENTO

REGISTRO OFICIAL®
ÓRGANO DE LA REPÚBLICA DEL ECUADOR

CONTRALORÍA GENERAL DEL ESTADO

ACUERDO N° 036-CG-2025

SE EXPIDE EL MANUAL DE AUDITORÍA INFORMÁTICA Y LA GUÍA TÉCNICA PARA LA REALIZACIÓN DE AUDITORÍAS INFORMÁTICAS

Año I - Nº 99 - 271 páginas
Quito, viernes 8 de agosto de 2025

ACUERDO No. 036-CG-2025

EL CONTRALOR GENERAL DEL ESTADO

CONSIDERANDO:

Que, el artículo 82 de la Constitución de la República del Ecuador, señala que el derecho a la seguridad jurídica se fundamenta en el respeto a la Constitución y en la existencia de normas jurídicas previas, claras, públicas y aplicadas por las autoridades competentes;

Que, conforme lo prescrito en el artículo 204, inciso tercero de la Carta Magna, la Contraloría General del Estado tiene personalidad jurídica y autonomía financiera, presupuestaria y organizativa; y, de conformidad con el artículo 211 ibidem "*…es un organismo técnico encargado del control de la utilización de los recursos estatales, y la consecución de los objetivos de las instituciones del Estado y de las personas jurídicas de derecho privado que dispongan de recursos públicos (…)*";

Que, el numeral 3 del artículo 212 de la Constitución de la República del Ecuador, establece como función de la Contraloría General del Estado, el expedir normativa para el cumplimiento de sus funciones;

Que, el artículo 226 ibidem, prescribe que "*Las instituciones del Estado, sus organismos, dependencias, las servidoras o servidores públicos y las personas que actúen en virtud de una potestad estatal ejercerán solamente las competencias y facultades que les sean atribuidas en la Constitución y la ley. Tendrán el deber de coordinar acciones para el cumplimiento de sus fines y hacer efectivo el goce y ejercicio de los derechos reconocidos en la Constitución.*";

Que, el artículo 227 de la Carta Magna, establece que "*La administración pública constituye un servicio a la colectividad que se rige por los principios de eficacia, eficiencia, calidad, jerarquía, desconcentración, descentralización, coordinación, participación, planificación, transparencia y evaluación.*";

Que, los numerales 5 y 31 del artículo 7, y numeral 22 del artículo 95 de la Ley Orgánica de la Contraloría General del Estado, facultan a la Entidad de Control la expedición de normativa para el funcionamiento del sistema de control, la práctica de la auditoría gubernamental y las demás que sean necesarias para el cumplimiento de sus funciones;

Que la Ley Orgánica de Prevención, Detección y Combate del Delito de Lavado de Activos y de la Financiación de otros delitos, en la Disposición Reformatoria Cuarta, reforma a la Ley Orgánica de la Contraloría General del Estado, agregando el artículo 23.3: "*Auditoría informática. - Se enfoca en el control de los recursos informáticos de las entidades, organismos del sector público y de las personas jurídicas de derecho privado que dispongan de recursos públicos para evaluar su eficiencia y efectividad. Esta modalidad de control examinará y verificará los sistemas, las aplicaciones, infraestructura y procesos de tecnología de la información para identificar y corregir vulnerabilidades, incumplimientos y riesgos que puedan afectar a la integridad, la confidencialidad, la disponibilidad de la información y los recursos informáticos, a fin de evitar fuga de información que pueda afectar a la integridad de los recursos públicos. Esta modalidad de auditoría concluirá con el informe correspondiente que contendrá los comentarios, conclusiones y recomendaciones pertinentes.*";

Que, la Ley Orgánica ibidem, expedida el 20 de junio de 2024 y publicada en el Cuarto Suplemento del Registro Oficial No. 610 de 29 de Julio 2024, en su Disposición Final Única establece que esta ley entrará vigencia en el plazo de un año posterior a su publicación el en Registro Oficial;

Que, la Disposición Reformatoria Cuarta de la Ley Orgánica de Integridad Pública, publicada en el Tercer Suplemento del Registro Oficial No. 68, de 26 de junio de 2025, reformó la Ley Orgánica de la Contraloría General del Estado, sustituyendo el artículo 39 por el siguiente: "…*Art. 39.- Determinación de responsabilidades y seguimiento.- A base de los resultados de la auditoría gubernamental, contenidos en actas o informes, la Contraloría General del Estado, tendrá potestad exclusiva para predeterminar o no y para determinar o no responsabilidades administrativas y civiles culposas, así como generar o no órdenes de reintegro, e indicios de responsabilidad penal de ser el caso. (…) De existir indicios de responsabilidad penal, se procederá de acuerdo a lo previsto en los artículos 65, 66 y 67 de esta Ley. - En todos los casos, la evidencia que sustente la determinación de responsabilidades, a más de suficiente, competente y pertinente, reunirá los requisitos formales para fundamentar la defensa en juicio. - La Contraloría General del Estado efectuará el seguimiento de la emisión y cobro de los títulos de crédito originados*…".

Que, la Agencia Francesa de Desarrollo (AFD), institución financiera pública que representa uno de los principales instrumentos de cooperación internacional en

Francia y cuya misión es luchar contra la pobreza y promover el desarrollo sostenible en los países en desarrollo, mantiene un acuerdo con la República del Ecuador para apoyar el diseño y la puesta en marcha de un nuevo programa de políticas públicas para la protección y el uso sostenible de las zonas marinas y costeras;

Que, según sus políticas y procedimientos internos, la Agencia Francesa de Desarrollo (AFD) realizó una evaluación de gasto público y rendición de cuentas a Ecuador, denominada *"Evaluación PEFA - limitada";*

Que, la Agencia Francesa de Desarrollo (AFD) apoya a la Contraloría General del Estado, con una Asistencia Técnica dedicada a tratar las debilidades identificadas en la Dimensión 4 (D4), que trata de "Supervisión y auditoría externas", con un enfoque en el Indicador ID 30 – Auditoría externa, en el proyecto "Asistencia técnica en apoyo al fortalecimiento del proceso de auditorías de la CGE", que incluye las modalidades de auditoría incorporadas por la Ley Orgánica de Prevención, Detección y Combate del Delito de Lavado de Activos y de la Financiación de otros Delitos;

Que, en ese contexto, la Contraloría General del Estado contó con la asistencia técnica de la Agencia Francesa de Desarrollo, AFD, para la elaboración de la Guía Técnica para la realización de las Auditorías Informáticas;

Que, mediante Acuerdo 015-CG-2020, de 30 de julio de 2020, publicado en la Edición Especial 852 del Registro Oficial, de 05 de agosto de 2020 y sus posteriores reformas, se expidió el Estatuto Orgánico de Gestión Organizacional por Procesos de la Contraloría General del Estado;

Que, mediante Acuerdo 012-CG-2021, de 13 de agosto de 2021, publicado en el Cuarto Suplemento del Registro Oficial No. 519, de 19 de agosto de 2021 y sus posteriores reformas, se expidió el Reglamento Sustitutivo de Suscripción de Documentos de la Contraloría General del Estado;

Que, mediante Acuerdo 028-CG-2023, de 22 de septiembre de 2023, publicado en el Registro Oficial No. 409, de 03 de octubre de 2023, se expidió el Reglamento de clasificación de información y/o documentación reservada en la Contraloría General del Estado;

Que, mediante Acuerdo 029-CG-2023, de 22 de septiembre de 2023, publicado en el Registro Oficial No. 413, de 10 de octubre de 2023, se expidió el Reglamento de clasificación de información y/o documentación de carácter confidencial en la Contraloría General del Estado;

Que, mediante Acuerdo 014-CG-2024, de 24 de abril de 2024, publicado en el Primer Suplemento del Registro Oficial No. 554, de 09 de mayo de 2024 y su

reforma, se expidió el Reglamento de Ámbito de Control de las Unidades Administrativas de la Contraloría General del Estado;

Que, mediante Acuerdo 039-CG-2024, de 09 de octubre de 2024, publicado en el Registro Oficial No. 669, de 22 de octubre de 2024, se expidió el Reglamento para Suscripción de Documentos con Firma Electrónica en la Contraloría General del Estado;

Que, mediante Acuerdo 002-CG-2025, de 21 de enero de 2025, publicado en el Cuarto Suplemento del Registro Oficial No. 727, de 22 de enero de 2025, se expidió el Reglamento de Determinación de Responsabilidades;

Que, mediante Acuerdo 012-CG-2025, de 05 de marzo de 2025, publicado en el Cuarto Suplemento del Registro Oficial No. 758, de 10 de marzo de 2025, se expidió el Reglamento para las notificaciones electrónicas que efectúa la Contraloría General del Estado;

Que, mediante Acuerdo 016-CG-2025, de 16 de abril de 2025, se expidió el Reglamento para la Elaboración, Trámite y Aprobación de Informes de Auditoría Gubernamental; y,

Que, es necesaria la actualización normativa sobre la base de disposiciones legales vigentes y necesidades institucionales, especialmente en el ámbito de la ejecución de las acciones de control.

En ejercicio de las facultades que le confiere el artículo 212, numeral 3 de la Constitución de la República del Ecuador, y artículos 95 y 31, numeral 23 de la Ley Orgánica de la Contraloría General del Estado,

ACUERDA:

EXPEDIR EL MANUAL DE AUDITORÍA INFORMÁTICA Y LA GUÍA TÉCNICA PARA LA REALIZACIÓN DE AUDITORÍAS INFORMÁTICAS

Art. 1.- Expídase el Manual de Auditoría Informática con sus respectivos anexos, que forma parte integrante del presente instrumento y que consta como Anexo 1.

Art. 2.- Expídase la Guía Técnica para la realización de Auditorías Informáticas con sus respectivos anexos, que forma parte integrante del presente Acuerdo y que consta como Anexo 2.

Art. 3.- El Manual de Auditoría Informática y la Guía Técnica para la realización de Auditorías Informáticas, serán de uso obligatorio para las acciones de control que en materia de informática realicen todas las unidades de auditoría de la Contraloría General del Estado.

DISPOSICIONES GENERALES

Primera. - Los servidores de la Contraloría General del Estado que intervengan en la recepción, trámite y emisión de los informes previstos en el Manual de Auditoría Informática y la Guía Técnica para la realización de Auditorías Informáticas del presente Acuerdo, deberán mantener estricta reserva y confidencialidad sobre toda la información y documentación a la que tengan acceso en el ejercicio de sus funciones. La entrega de información y/o documentación que como resultado de la acción de control contenga o se refiera a información confidencial y/o reservada, se sujetará a la Constitución de la República del Ecuador, la Ley y la normativa aplicable emitida para el efecto.

Segunda. – Encárguese de la ejecución del presente Acuerdo, al Subcontralor/a de Auditoría y demás titulares de las unidades administrativas determinadas por dicha autoridad como responsables de la aplicación del presente Acuerdo, para lo cual implementarán controles permanentes a sus procesos, y actividades y aplicativos informáticos, a fin de garantizar el cumplimiento de las disposiciones constitucionales y legales, la observancia del debido proceso, el cumplimiento de plazos y términos legales y de la normativa aplicable. De evidenciarse incumplimientos, estos serán comunicados por los citados titulares al Contralor/a General del Estado, mediante un informe motivado y con la documentación de sustento, para que adopte las acciones respectivas.

Tercera. - Las unidades de auditoría de la Contraloría General del Estado, deberán observar el "*Catálogo de Formatos para aplicación operativa del Reglamento para la elaboración, trámite y aprobación de informes de auditoría gubernamental*", así como también los anexos que constan tanto el Manual de Auditoría Informática como en la Guía Técnica de Auditoría Informática, para su correspondiente aplicación.

DISPOSICIÓN DEROGATORIA

Se derogan todas las normas, disposiciones, instructivos y demás instrumentos jurídicos de igual o menor jerarquía que se contrapongan a lo dispuesto en el presente Acuerdo.

DISPOSICIÓN FINAL

El presente Acuerdo entrará en vigencia a partir del 29 de julio de 2025, sin perjuicio su publicación en el Registro Oficial.

Dado, en el Despacho del Contralor General del Estado, en la ciudad de San Francisco de Quito, Distrito Metropolitano, a los veinticinco días del mes de julio de dos mil veinticinco.

Comuníquese. –

Firmado electrónicamente por:
XAVIER MAURICIO TORRES MALDONADO
Validar únicamente con FirmaEC

Dr. Mauricio Torres M., PHD
CONTRALOR GENERAL DEL ESTADO

CONTRALORÍA GENERAL DEL ESTADO. – SECRETARÍA GENERAL. - Dictó y firmó electrónicamente el Acuerdo que antecede, el doctor Mauricio Torres M., PhD, Contralor General del Estado, en la ciudad de San Francisco de Quito, Distrito Metropolitano, a los veinticinco días del mes de julio de dos mil veinticinco. LO CERTIFICO.

Firmado electrónicamente por:
MARCELO FERNANDO MANCHENO MANTILLA
Validar únicamente con FirmaEC

Dr. Marcelo Mancheno Mantilla
SECRETARIO GENERAL

ANEXO 1

MANUAL DE AUDITORÍA INFORMÁTICA

PRESENTACIÓN

El presente documento tiene por objeto poner a disposición del auditor informático un instrumento de trabajo con lineamientos que faciliten la ejecución de la auditoría a los procesos, sistemas de información, aplicaciones, infraestructura tecnológica, seguridad de la información, así como sus adquisiciones, en instituciones y organismos del sector público; y, entidades del sector privado que disponen de recursos públicos, sujetos al control de la Contraloría General del Estado.

Para lograr un mejor entendimiento de los procedimientos a aplicar por el auditor informático, el contenido de este manual se ha estructurado en tres capítulos, que se describen a continuación:

El capítulo 1 contiene la parte introductoria del manual y describe, sus objetivos generales y específicos, el marco legal y normativo aplicable, sustentado en las disposiciones constitucionales, leyes orgánicas y normas técnicas que rigen el control con énfasis en las tecnologías de la información y comunicaciones, además se han considerado estándares y marcos de referencia internacionales aplicables a la materia; así como, las funciones y responsabilidades del personal técnico que participa en las auditorías informáticas y en acciones de control de otra naturaleza.

El capítulo 2 desarrolla el concepto de auditoría informática, su alcance, objetivos generales y específicos, principios fundamentales y ámbitos de aplicación; así también, se definen componentes y los elementos claves que el auditor debe considerar para la ejecución de su trabajo.

En el capítulo 3 se describen los contenidos técnico, administrativo y documental de las fases de la auditoría: planificación, ejecución, elaboración y trámite de aprobación del informe de auditoría. Además, se aborda el procedimiento a seguir para la comunicación de resultados provisionales.

Finalmente se incluyen las siglas y abreviaturas utilizadas, un glosario de términos, anexos y las referencias bibliografías utilizados en la elaboración del presente manual.

ÍNDICE

PRESENTACIÓN

ÍNDICE

CAPÍTULO 1

1. INTRODUCCIÓN
2. OBJETIVOS DEL MANUAL
2.1. OBJETIVOS GENERALES
2.2. OBJETIVOS ESPECÍFICOS
3. MARCO LEGAL Y NORMATIVO
4. FUNCIONES Y RESPONSABILIDADES

CAPÍTULO 2

2. AUDITORÍA INFORMÁTICA
2.1. DEFINICIÓN
2.2. ALCANCE DE LA AUDITORÍA INFORMÁTICA
2.3. OBJETIVOS
2.3.1. Objetivo General
2.3.2. Objetivos Específicos
2.4. PRINCIPIOS FUNDAMENTALES
2.5. ÁMBITO DE APLICACIÓN DE LA AUDITORÍA INFORMÁTICA
2.5.1. Gestión informática
2.5.2. Seguridad de TI
2.5.3. Infraestructura tecnológica
2.5.4. Sistemas o Aplicativos
2.5.5. Adquisiciones tecnológicas
2.6. COMPONENTES PARA EL ANÁLISIS EN LA AUDITORÍA INFORMÁTICA
2.6.1. Gobernanza y Gestión de TI
2.6.2. Desarrollo y Adquisición de TI
2.6.3. OPERACIONES DE TI
2.6.4. Externalización
2.6.5. Gestión de la Continuidad del Negocio
2.6.6. Seguridad de la Información
2.6.7. Controles de Aplicación

CAPÍTULO 3

3. PROCESO DE LA AUDITORÍA INFORMÁTICA
3.1. FASE DE PLANIFICACIÓN
3.1.1. Planificación general
3.1.2. Control Interno

3.1.2.1. Evaluación al sistema de control interno
3.1.2.2. Seguimiento al cumplimiento de recomendaciones
3.1.3. Riesgos de Auditoría
3.1.4. Pruebas y Técnicas
3.1.5. Documento de planificación
3.2. EJECUCIÓN DE LA AUDITORÍA
3.2.1. Consideraciones previas en la ejecución de la Auditoría de TI
3.2.2. Pruebas de auditoría de TI.
3.2.3. Hallazgos de Auditoría
3.2.4. Elementos del Hallazgo de Auditoría
3.2.5. Evidencia de Auditoría
3.2.6. Conclusiones de Auditoría
3.2.7. Papeles de Trabajo
3.3. COMUNICACIÓN DE RESULTADOS PROVISIONALES
3.4. INFORME DE AUDITORÍA

SIGLAS Y ABREVIATUAS UTILIZADAS

GLOSARIO DE TÉRMINOS

REFERENCIAS BIBLIOGRÁFICAS

ANEXOS

CAPÍTULO 1

1. INTRODUCCIÓN

La Contraloría General del Estado (CGE), en su calidad de Organismo Técnico de Control y Entidad Fiscalizadora Superior (EFS), tiene entre sus atribuciones la fiscalización del uso de los recursos públicos, incluidos los recursos informáticos de las entidades, organismos del sector público y de las personas jurídicas de derecho privado que dispongan de recursos públicos para evaluar su eficiencia y efectividad.

La creciente adopción de Tecnologías de la Información y la Comunicación (TIC) en el sector público ha transformado de manera significativa los procesos institucionales, convirtiéndose en un factor clave para el fortalecimiento del control gubernamental. En este contexto, la implementación de soluciones tecnológicas, tanto a nivel de sistemas de información como de infraestructura, exige mecanismos de supervisión que garanticen su uso eficiente, seguro y transparente.

El constante desarrollo de la tecnología de la información y la comunicación ha hecho posible capturar, almacenar, procesar y entregar información en forma electrónica; esta transición ha generado un cambio significativo en el entorno operativo al que debe responder la CGE; por otra parte, se suma el crecimiento sostenido del gasto público en TI, lo que hace imprescindible que la CGE fortalezca sus capacidades para realizar auditorías informáticas efectivas.

En respuesta a esta realidad, la CGE ha desarrollado competencias especializadas para llevar a cabo auditorías informáticas orientadas a evaluar la eficiencia, eficacia, seguridad y confiabilidad de los sistemas, plataformas y componentes tecnológicos que respaldan la gestión pública.

En las auditorías informáticas se examinará y verificará los sistemas, aplicaciones, infraestructura y procesos tecnológicos, con el fin de identificar y mitigar vulnerabilidades, incumplimientos y riesgos que puedan afectar a la integridad, la confidencialidad, la disponibilidad de la información y los recursos informáticos, de este modo, se busca prevenir la fuga de información y salvaguardar los recursos públicos.

2. OBJETIVOS DEL MANUAL

2.1. Objetivos generales

El manual de auditoría informática tiene los siguientes objetivos generales:

- Establecer directrices a los equipos de auditoría de la Contraloría General del Estado (CGE) en los procesos de planificación, ejecución, comunicación de resultados provisionales y elaboración del informe en auditorías informáticas.

- Garantizar independencia, aplicación de criterios técnicos y generación de valor público, como resultado de la realización de auditorías informáticas a los sistemas, aplicaciones, infraestructura y procesos de tecnología de la información y comunicaciones.

- Proporcionar un instrumento para efectuar el control de los recursos informáticos de las entidades, que permita identificar vulnerabilidades, evaluar riesgos y verificar la correcta implementación de controles internos, asegurando así su eficiencia, efectividad, seguridad y cumplimiento normativo.

2.2. Objetivos específicos

Los objetivos específicos son los siguientes:

- Guiar al equipo auditor en la ejecución de los procedimientos para determinar que la gestión de las tecnologías de la información esté alineada a la planificación estratégica, planes operativos y de contratación de la entidad; así como, que contribuyen e impulsan el logro de los objetivos institucionales.

- Proporcionar lineamientos para que la auditoría informática evalúe que las acciones implementadas por la entidad, salvaguarde la confidencialidad, integridad y disponibilidad de la información; así como, garantice el funcionamiento seguro y eficiente de los sistemas.

- Proveer al equipo auditor herramientas que permitan verificar que la entidad dispone de una arquitectura e infraestructura tecnológica que soporte los sistemas informáticos institucionales; además, de planes que garanticen las operaciones tecnológicas ante interrupciones críticas, desastres naturales o ciberataques.

- Proporcionar lineamientos para examinar que el software utilizado por la institución, cumple con los requerimientos normativos, funcionales y técnicos, para la generación de información confiable y que contribuya al desarrollo de sus funciones, atribuciones y logro de objetivos.

- Establecer un marco claro y sistemático que permita al equipo auditor evaluar las adquisiciones tecnológicas conforme los principios y normativa de contratación pública; garantizando el uso óptimo de los recursos públicos.

3. MARCO LEGAL Y NORMATIVO

La acción fiscalizadora sólo es legítima cuando se cuenta y aplica un marco normativo claro, que delimita competencias, confiere potestades y establece obligaciones, por lo que, el presente manual, observa las disposiciones constitucionales, leyes orgánicas y normas técnicas que rigen el control con énfasis en las tecnologías de la información, además, considera los estándares y marcos de referencia internacionales aplicables a la materia, que son necesarios para la protección de datos, seguridad y disponibilidad de la información, así como prácticas de ciberseguridad para la prevención de accesos no autorizados; este anclaje jurídico, garantiza que los procedimientos de auditoría informática efectuados por la CGE y sus conclusiones, sean conocidos y entendidos por las partes interesadas, incuestionables ante los órganos de justicia, y proporcionen una base objetiva para disponer la corrección de las deficiencias detectadas.

En tal virtud, se ha definido la Normativa Nacional e Internacional aplicable incluyéndose los marcos de referencia, que se detalla en el anexo adjunto a este manual.

Anexo 1. – Marco Legal y Normativo

4. FUNCIONES Y RESPONSABILIDADES

A más de las funciones establecidas en los estatutos y manuales que se emitan para la administración del talento humano, los integrantes del equipo de auditoría cumplirán con las actividades que a manera de anexo se adjunta a este manual.

Anexo 2. – Funciones y responsabilidades

CAPÍTULO 2

2. AUDITORÍA INFORMÁTICA

2.1. DEFINICIÓN

La auditoría informática o auditoría de tecnología de la Información (TI) es un proceso sistemático de evaluación del uso que una entidad hace de sus recursos tecnológicos; lo que permitirá asegurar que el desarrollo, implementación y mantenimiento de los sistemas estén alineados con los objetivos de la entidad, y protejan los activos de información. Este proceso busca promover la eficiencia, la eficacia, la seguridad y el cumplimiento de las políticas internas y externas pertinentes.

2.2. ALCANCE DE LA AUDITORÍA INFORMÁTICA

El alcance de la auditoría informática incluye la revisión integral de todos los elementos relacionados con el uso de tecnologías de la información en una entidad. Esto abarca políticas, proyectos, procesos, procedimientos, infraestructura tecnológica, aplicaciones utilizadas, datos e información gestionada, así como las adquisiciones relacionadas con las operaciones de TI. El propósito es verificar que los sistemas y controles tecnológicos respondan adecuadamente a los requerimientos institucionales, garantizando su eficiencia, seguridad, confidencialidad, integridad y conformidad con la normativa vigente.

Sin embargo, debido a que las tecnologías de la información están estrechamente vinculadas con los procesos institucionales, la auditoría informática debe complementarse con otras ramas de auditoría, para ello, es fundamental la participación de equipos multidisciplinarios, integrados por

profesionales con conocimientos en áreas como administración, finanzas, operaciones y normativas sectoriales; este enfoque combinado permite analizar de forma integral los procesos, no solo desde la perspectiva tecnológica, sino también desde su impacto funcional, operativo y estratégico en la entidad.

Adicionalmente, dentro del alcance y modalidades de la Auditoría Gubernamental pueden identificarse componentes tecnológicos asociados a los procesos evaluados, en tales casos, se requiere un análisis técnico especializado, aplicando las directrices y metodologías descritas en el presente manual, con el fin de profundizar en los aspectos informáticos que puedan influir en los resultados del control.

2.3. OBJETIVOS

2.3.1. Objetivo General

Estandarizar la ejecución de auditorías de TI mediante la sistematización de procedimientos y la adopción de criterios y terminología uniformes. Esto proporciona a los auditores una metodología clara de trabajo que facilite la aplicación coherente de normas generales y específicas, así como del marco legal aplicable, garantizando una función de control con altos estándares profesionales.

2.3.2. Objetivos Específicos

- Ejecutar auditorías informáticas de forma estructurada y coherente, aplicando normas y procedimientos actualizados para examinar tanto los sistemas de información como la infraestructura que los soporta.

- Proponer procedimientos técnicos que respalden actividades de control con altos niveles de calidad y eficiencia, apoyados en herramientas modernas.

- Establecer objetivos de control que guíen la ejecución de pruebas de cumplimiento y pruebas sustantivas.

- Evaluar los controles clave de los procesos y sistemas de información que respaldan los objetivos institucionales.

- Realizar auditorías con personal con competencia técnica para realizar la auditoría con conocimientos y habilidades apropiados en TI, y emitir un dictamen independiente sobre la razonabilidad de las operaciones del sistema y la gestión administrativa del área de TI.

2.4. PRINCIPIOS FUNDAMENTALES

La auditoría informática debe observar los siguientes principios fundamentales, los que permitirán asegurar su calidad y efectividad, contribuyendo a la seguridad y la confianza en los sistemas de información:

- *Objetividad:* el auditor informático debe ser imparcial y neutral en la evaluación de los recursos de TI y procesos informáticos. No debe tener prejuicios o intereses personales que puedan afectar su juicio.

- *Independencia:* el auditor debe estar libre de conflictos de interés con las áreas y personas relacionadas con la auditoría.

- *Enfoque basado en riesgos:* la auditoría debe priorizar la evaluación de sistemas, procesos o controles que representen mayores riesgos para la confidencialidad, integridad y disponibilidad de la información. Esto permite un uso eficiente de los recursos disponibles.

- *Cobertura:* alcance efectivo que tiene la auditoría sobre los procesos, sistemas y aplicativos, infraestructura y controles tecnológicos de una entidad.

- *Confidencialidad:* obligación ética y profesional del auditor; así como, el compromiso de no divulgar información sensible obtenida durante el proceso de auditoría.

- *Ética:* el auditor debe observar el Código de Ética de la CGE, lo establecido en la NCI 407-08; normas y valores morales que guían el comportamiento profesional del auditor, para asegurar el comportamiento honesto, y profesional durante todas las fases del proceso de auditoría.

- *Competencia técnica:* capacidad, conocimientos actualizados, habilidades y experiencia que debe tener un auditor informático para realizar su trabajo de manera eficaz, confiable y conforme a la normativa y aplicación de buenas prácticas y estándares profesionales.

- *Normatividad:* el auditor debe cumplir con las normas y regulaciones aplicables a la auditoría informática. Esto puede incluir regulaciones locales, nacionales y mejores prácticas internacionales.

- *Evidencia:* toda conclusión del auditor debe estar respaldada por evidencia suficiente, competente y pertinente. Esta evidencia puede ser documental, digital, testimonial o basada en pruebas realizadas directamente sobre los sistemas.

2.5. ÁMBITO DE APLICACIÓN DE LA AUDITORÍA INFORMÁTICA

Para orientar adecuadamente los esfuerzos de control y evaluación en el área de tecnologías de la información, es necesario contar con una clasificación

clara que facilite la planificación de auditorías según los riesgos, prioridades institucionales y objetivos de gestión.

Cada clasificación de auditoría tiene un enfoque específico, ya sea técnico, operativo, normativo o estratégico, por lo que su correcta identificación permite asignar recursos, competencias y metodologías apropiadas para cada caso, así como, definir con precisión el alcance de la revisión, los equipos responsables, los componentes a evaluar y los resultados obtenidos. Dependiendo del alcance y los objetivos de la auditoría los ámbitos de aplicación pueden ser:

2.5.1. Gestión informática

Como parte de la auditoría informática comprende el análisis de la gestión de TI, su objetivo principal es determinar su alineamiento con los objetivos estratégicos institucionales, cumple con normativas internas y externas, y aplica principios de eficiencia, eficacia, economía y transparencia.

Este tipo de auditoría se enfoca en aspectos clave como la gobernanza de TI, la gestión de riesgos tecnológicos, la planificación estratégica del área de sistemas, el uso de recursos financieros y humanos, la contratación de servicios tecnológicos, y la calidad de los servicios entregados a los usuarios internos.

2.5.2. Seguridad de TI

Esta auditoría se aplica a todos los aspectos relacionados con la seguridad a partir de los activos de información como los sistemas informáticos dentro de la institución, incluyendo infraestructura, personal, procesos y áreas específicas. Su objetivo es evaluar las acciones preventivas, correctivas y detectivas implementadas para proteger los activos de información y garantizar el funcionamiento seguro y eficiente de los sistemas. Se examinan las políticas y controles establecidos para salvaguardar la confidencialidad, integridad y disponibilidad de la información, así como la gestión de accesos, autenticación,

cifrado, incidentes de seguridad, políticas de contraseñas, respaldos, protección antivirus y el uso de controles de acceso, entre otros.

2.5.3. Infraestructura tecnológica

Esta auditoría se enfoca en evaluar la arquitectura tecnológica que sostiene los sistemas informáticos institucionales, incluyendo servidores, redes, equipos de cómputo, sistemas operativos, dispositivos de almacenamiento y equipamiento de los centros de datos. Se analiza si la infraestructura está correctamente dimensionada, actualizada y operativa, y si garantiza la disponibilidad, continuidad y rendimiento del servicio. Además, se verifica si la institución cuenta con un Plan de Continuidad del Negocio (BCP) y un Plan de Recuperación ante Desastres (DRP) que le permitan mantener o reanudar sus operaciones tecnológicas ante interrupciones críticas, desastres naturales o ciberataques, pruebas de recuperación, responsabilidades asignadas, tiempos de recuperación (RTO) y niveles aceptables de pérdida de datos (RPO). En este contexto, también se examinan los respaldos, la existencia y operatividad de centros alternos de datos, así como las estrategias implementadas para minimizar el impacto de posibles contingencias.

2.5.4. Sistemas o Aplicativos

Este tipo de auditoría es un proceso sistemático de evaluación orientado a revisar la funcionalidad, integridad, seguridad y eficiencia de los sistemas de información utilizados por una entidad. Esta auditoría se enfoca en los aplicativos informáticos que automatizan procesos, se centra en evaluar integralmente los sistemas de software, su diseño, desarrollo, implementación, operación y mantenimiento. Analiza si las aplicaciones cumplen con los requerimientos normativos, funcionales y técnicos definidos, si permiten la trazabilidad de la información, generan reportes confiables.

Examina el manejo y estructura de las bases de datos asociadas, evaluando la clasificación de los datos, sus niveles de seguridad, confidencialidad y propiedad. La auditoría también considera el control de cambios, la documentación técnica, el soporte brindado y las prácticas de mantenimiento aplicadas. Se incluye la revisión del código fuente del software, verificando su calidad y estándares de desarrollo.

2.5.5. Adquisiciones tecnológicas

Evalúa la legalidad, pertinencia y eficiencia de las contrataciones relacionadas con tecnología de la información y comunicación, revisa todo el ciclo de adquisición, desde la planificación y definición de requerimientos hasta la contratación, recepción, implementación y uso de los recursos tecnológicos. Se enfoca en analizar aspectos como la pertinencia de las especificaciones técnicas o términos de referencia, la objetividad en los procesos de selección de proveedores, la calidad de los bienes y servicios entregados, el cumplimiento contractual, y la alineación de las adquisiciones con las necesidades institucionales. Se verifica si los procesos se realizaron conforme a la normativa vigente establecida por el ente rector de la contratación pública.

2.6. COMPONENTES PARA EL ANÁLISIS EN LA AUDITORÍA INFORMÁTICA

La definición de los componentes para la auditoría informática, permite delimitar el alcance, orientar el análisis técnico y enfocar los recursos de manera efectiva, a fin de garantizar que el proceso de auditoría sea ordenado y completo. A continuación, se describe los componentes considerados para fines de este manual:

2.6.1. Gobernanza y Gestión de TI

Constituye el marco general que orienta las operaciones tecnológicas de una entidad para asegurar que estas respondan a las necesidades actuales y futuras

de la institución. Forma parte integral de la gobernanza organizacional e incluye el liderazgo, las estructuras, procesos y mecanismos institucionales que garantizan que los sistemas de TI respalden los objetivos estratégicos, gestionen adecuadamente los recursos y mitiguen los riesgos. Esto abarca aspectos como el cumplimiento de normas, la elaboración de informes, la retroalimentación, y la asignación de recursos tecnológicos. En el ámbito de la auditoría informática el análisis de la Gobernanza, comprende la evaluación de la satisfacción de las necesidades tecnológicas de las partes interesadas para alcanzar los objetivos institucionales.

Elementos clave para la gobernanza y gestión de TI

a) Estrategia y planificación de TI

Define cómo la tecnología de la información se alineará con sus objetivos institucionales, asegurando el uso eficiente, seguro y sostenible de los recursos tecnológicos. Este proceso incluye la elaboración de planes estratégicos operativos y de adquisiciones, alineados a los objetivos estratégicos institucionales y políticas de gobierno.

b) Estructuras, normas, políticas y procesos institucionales

Las estructuras, normas, políticas internas y externas, y procesos institucionales son elementos interconectados para el funcionamiento de la entidad y alcanzar sus objetivos. Las estructuras establecen la forma en que se divide el trabajo y se distribuyen las responsabilidades. Las normas son reglas específicas que guían el comportamiento de los miembros y regulan los procesos. Las políticas son directrices generales que orientan la toma de decisiones. Los procesos describen las acciones secuenciales para lograr un resultado específico.

En conjunto, estos elementos aseguran la coherencia, eficiencia y cumplimiento de los objetivos institucionales.

c) Gestión de los recursos humanos de TI

Las áreas de tecnologías de la información (TI) deben contar con políticas de talento humano actualizadas y alineadas con los objetivos organizacionales. Es fundamental definir claramente los perfiles y requisitos de los cargos, así como asegurar que el personal cumpla con las competencias profesionales necesarias. La formación continua a través de planes de capacitación y desarrollo, junto con evaluaciones periódicas de desempeño, contribuye al fortalecimiento del equipo de TI. Además, es importante considerar los riesgos asociados a la segregación de funciones y garantizar la disponibilidad de personal de reemplazo para los puestos clave, asegurando así la continuidad operativa y la eficiencia del área.

d) Gestión de riesgos de TI

Comprende la identificación, análisis y evaluación de los riesgos asociados a las aplicaciones, la infraestructura y los servicios de Tecnologías de la Información, así como a la información generada, procesada y almacenada por estos medios. Incluye además una gestión continua, que contempla la revisión periódica de los riesgos identificados y la verificación de la efectividad de las estrategias de mitigación implementadas.

2.6.2. Desarrollo y Adquisición de TI

El desarrollo y la adquisición de TI se refieren a los procesos de creación y compra de tecnología de la información, respectivamente. El desarrollo de TI implica la creación de sistemas y aplicaciones de software, mientras que la adquisición de TI se centra en la compra de hardware, software y servicios de TI para satisfacer las necesidades de una entidad.

Tanto el desarrollo como la adquisición de TI son estrategias importantes para las instituciones que buscan mejorar su eficiencia y competitividad a través de

la tecnología. La elección entre ambas dependerá de las necesidades, recursos y objetivos específicos de cada institución.

Elementos clave del desarrollo y adquisición de TI

a) Estudio de factibilidad

Todo desarrollo y/o adquisición de TI previo a la definición de requisitos contemplará un estudio de factibilidad con el fin de analizar los beneficios y soluciones a desarrollar y determinar su viabilidad.

b) Desarrollo y gestión de requisitos

Es el proceso mediante el cual se identifican, documentan, analizan, validan y gestionan las necesidades funcionales y no funcionales que debe cumplir una solución tecnológica. Este proceso es esencial para asegurar que los sistemas, aplicaciones o servicios implementados respondan efectivamente a los objetivos de la organización y a las expectativas de los usuarios.

c) Gestión y control de proyectos

La gestión y control de proyectos de TI comprende el conjunto de prácticas, procesos y herramientas aplicadas para planificar, ejecutar, monitorear y cerrar proyectos tecnológicos, con el objetivo de asegurar que se entreguen los productos a tiempo, dentro del presupuesto, con la calidad esperada y alineados con los objetivos estratégicos institucionales.

d) Diseño/Desarrollo

El diseño y desarrollo en el contexto de Tecnologías de la Información (TI) comprende las etapas en las que se definen, estructuran, construyen y prueban soluciones tecnológicas, como aplicaciones, sistemas, bases de datos,

componentes o integraciones, en función de los requerimientos funcionales y no funcionales previamente establecidos.

Una vez definidos los requerimientos de la solución tecnológica en esta etapa se establecen las especificaciones de software, hardware y medios de conectividad, necesarios para el funcionamiento integral y despliegue de la solución tecnológica para su utilización.

e) Aseguramiento de la calidad y pruebas

El aseguramiento de la calidad y las pruebas en TI comprende el conjunto de actividades orientadas a verificar que los sistemas, aplicaciones y servicios tecnológicos cumplan con los requisitos funcionales, técnicos y de seguridad, antes de ser implementados en producción. Estas actividades buscan garantizar la confiabilidad, integridad, desempeño y seguridad de las soluciones tecnológicas, minimizando errores, fallos y riesgos operativos.

f) Gestión de la configuración

La gestión de la configuración es el proceso mediante el cual una entidad identifica, registra, controla y mantiene actualizada la información sobre los componentes tecnológicos (activos de configuración) que conforman su infraestructura de TI, incluyendo sus versiones, relaciones y estados. Su objetivo es asegurar la integridad, trazabilidad y control de los sistemas y servicios tecnológicos, permitiendo una gestión eficiente de cambios, incidentes, activos y mantenimientos.

g) Adquisición de Infraestructura tecnológica

Comprende el proceso mediante el cual una organización planifica, evalúa, selecciona y adquiere componentes físicos y virtuales necesarios para soportar sus operaciones y servicios de TI. Esta infraestructura incluye, entre otros: servidores, equipos de cómputo, redes, almacenamiento, dispositivos de

seguridad, virtualización y componentes de centros de datos. Este proceso debe ejecutarse de manera planificada, transparente y alineada con las necesidades institucionales, considerando criterios de eficiencia, escalabilidad, compatibilidad, seguridad y sostenibilidad.

2.6.3. Operaciones de TI

Comprenden las actividades necesarias para mantener y brindar soporte a la infraestructura tecnológica de una entidad. Esto incluye procedimientos y controles para la administración, operación, soporte de los servicios y recursos tecnológicos de una entidad, con la finalidad de asegurar la disponibilidad de los sistemas e infraestructura, la gestión oportuna de incidentes, resolución de problemas, mantenimiento de configuraciones, control de cambios y monitoreo del desempeño de los servicios tecnológicos.

Elementos clave para las Operaciones de TI

a) Gestión de la Capacidad

Permite asegurar que la infraestructura, servicios y recursos de TI puedan soportar las necesidades institucionales actuales y futuras en términos de procesamiento, almacenamiento, red y rendimiento de manera eficiente y rentable, garantizando además, que los servicios de TI tengan suficiente capacidad de procesamiento, almacenamiento, conectividad y rendimiento para cumplir con los acuerdos de nivel de servicio (SLA), para lo cual es necesario que se verifique que se cuente con la estimación de las condiciones y necesidades actuales para tomar aquellas medidas que facilitan el suministro de las capacidades requeridas para mantener la disponibilidad de los sistemas y servicios TI.

Este proceso busca anticiparse a la demanda, optimizar el uso de recursos y garantizar que el rendimiento de los servicios tecnológicos se mantenga dentro de los niveles aceptables, evitando sobrecargas, caídas o subutilización.

b) Gestión de Cambios

Es un proceso formal que tiene como objetivo controlar, coordinar y autorizar cualquier modificación en la infraestructura tecnológica, aplicaciones, sistemas o servicios, asegurando que dichos cambios sean planificados, evaluados, aprobados, implementados y revisados de manera controlada, con el fin de minimizar riesgos, evitar interrupciones y garantizar la continuidad operativa.

c) Gestión de Incidentes y problemas

Es el conjunto de procesos destinados a garantizar la continuidad, calidad y eficiencia de los servicios de TI, mediante la atención estructurada de interrupciones, fallos, solicitudes y causas raíz que afectan el funcionamiento normal de los sistemas tecnológicos.

Su objetivo es restablecer la operación normal en el menor tiempo posible, minimizar el impacto sobre los usuarios y prevenir la recurrencia de errores o incidentes mayores, asegurando así la estabilidad y confiabilidad de los servicios tecnológicos ofrecidos por la organización.

d) Gestión de Servicios

Comprenden los SLA acordados por la entidad para asegurar que estos servicios cumplan con parámetros previamente establecidos de disponibilidad, tiempo de respuesta, capacidad y soporte, si los usuarios se encuentran satisfechos y se están tomando las medidas adecuadas en el caso de registrarse desviaciones respecto de los parámetros del nivel de servicio acordados. Estos parámetros incluyen medidas cuantificables, como la disponibilidad, utilización o número de errores.

e) Gestión de Activos de TI

Proceso mediante el cual se identifican, registran, controlan y supervisan los activos tecnológicos a lo largo de su ciclo de vida, a fin de garantizar un uso eficiente y seguro de acuerdo a las políticas institucionales.

2.6.4. Externalización

Conocida como outsourcing, se refiere al proceso mediante el cual una Entidad contrata a un proveedor externo para que gestione total o parcialmente sus funciones, servicios o infraestructura tecnológica.

Se evalúa mediante indicadores clave de desempeño (KPI), que permiten medir su eficacia. Los estándares de servicio suelen definirse en acuerdos de nivel de servicio (SLA) y Contrato de soporte (UC) pactados entre el área de TI y proveedores, los cuales deben ser monitoreados y revisados continuamente para asegurar el cumplimiento de los compromisos establecidos.

Esto puede incluir: soporte técnico y help desk, servicios de almacenamiento y backup en la nube, hosting y mantenimiento de servidores y aplicaciones, desarrollo y pruebas de software, servicios de seguridad y ciberseguridad (SOC, antivirus gestionado), gestión de redes o bases de datos, instalación, mantenimiento y provisión de equipos de computación y redes relacionadas.

Elementos clave de externalización

a) Cumplimiento legal y normativo

Comprende la verificación del cumplimiento de leyes emitidas por los entes rectores de la contratación pública, de protección de datos personales, para uso de servicios en la nube en el sector público y otras disposiciones relacionadas con la seguridad de la información, propiedad intelectual, confidencialidad y uso de recursos públicos.

2.6.5. Gestión de la Continuidad del Negocio

Garantizar la disponibilidad y recuperación de los servicios tecnológicos críticos ante interrupciones imprevistas; por lo que, incorpora un conjunto de planes, estrategias y procedimientos técnicos y organizativos que aseguran que los

sistemas de TI puedan seguir operando o ser recuperados rápidamente ante situaciones como: fallos de hardware o software, ataques cibernéticos (ransomware, DDoS), errores humanos, desastres naturales, cortes de energía o fallos de red.

Elementos clave para la gestión de la continuidad del negocio

a) Política, plan y organización de la continuidad del negocio

Define los objetivos generales para la continuidad de las operaciones de la institución, en ella se establece el marco y las responsabilidades institucionales relativas a la planificación de dicha continuidad.

2.6.6. Seguridad de la Información

La seguridad de la información se refiere a la protección de los datos y sistemas frente a accesos no autorizados, usos indebidos, divulgaciones no deseadas, alteraciones o destrucciones. Su objetivo es garantizar la confidencialidad, integridad y disponibilidad de la información.

Comprende la implementación de controles físicos, lógicos, de acceso, políticas de seguridad y concienciación del personal interno y externo de la organización sobre sus responsabilidades en el manejo de información sensible.

Además, la seguridad de la información contempla a la ciberseguridad la cual se enfoca en la protección frente a ciberataques, incluye políticas, normas y prácticas destinadas a reducir vulnerabilidades, asegurar la resiliencia ante incidentes y garantizar la recuperación operativa.

Elementos clave para la seguridad de la información

a) Evaluación de Riesgos de Seguridad de la Información

La gestión de riesgos en el ámbito de las tecnologías de la información debe incluir un proceso formalizado para la evaluación de riesgos de seguridad de la

información, asegurando su aplicación efectiva dentro de la organización. Este enfoque permite identificar, analizar y mitigar amenazas relacionadas con la seguridad, la ciberseguridad, la continuidad del negocio y la privacidad. Asimismo, es esencial que estos riesgos estén integrados al mapa general de riesgos de TI, lo que facilita una visión integral y coherente para la toma de decisiones estratégicas y operativas.

b) Política de Seguridad de la Información

Es un documento estratégico que define las reglas, responsabilidades y directrices para proteger los activos de información de una entidad. Es fundamental para asegurar la confidencialidad, integridad y disponibilidad de la información, y sirve como marco para implementar controles técnicos, físicos y administrativos, para lo cual se debe evaluar si existe orientación estratégica y respaldo adecuados respecto a la seguridad de la información en términos de una política de seguridad, su cobertura, la concientización y su cumplimiento por parte de toda entidad.

c) Organización de la Seguridad de TI

Comprende la estructura conformada por una o más personas quienes serán los responsables de la implementación de las políticas y procedimientos de seguridad informática y de la información, coordinar con las unidades en especial con las que administran las tecnologías, los responsables de la información generada en los procesos de la entidad para la implementación de los controles, capacitar al personal técnico y usuarios de los sistemas acerca del uso responsable de la información y gestión de incidentes, así como, la implementación de mecanismos de seguridad para la transferencia e intercambio de información con entes externos a la entidad.

d) Gestión de Activos de Información

Comprende la identificación, valoración, clasificación y protección de los activos clave de información en relación a su importancia para la entidad, que

aseguren la protección de la información, cumplimiento normativo, continuidad del negocio y mejora de la eficiencia de los procesos.

e) Seguridad física y del entorno

Comprende la definición de las medidas e implementación de controles para proteger los activos de información y las instalaciones que los albergan contra amenazas físicas. Esto incluye la protección contra accesos no autorizados, daños, interrupciones y desastres naturales, con la finalidad de proteger los activos de información, cumplimiento normativo, asegurar la disponibilidad y continuidad de los servicios de TI y operaciones de la entidad y reducción de riesgos.

f) Control de Accesos

Comprende las políticas, procedimientos, mecanismos y herramientas que regulan el ingreso, uso y manejo de los recursos tecnológicos, tanto físicos como lógicos. Su propósito es asegurar que únicamente las personas debidamente autorizadas puedan acceder a sistemas, aplicaciones, redes, bases de datos o infraestructuras críticas, en función de sus roles y responsabilidades, garantizando la confidencialidad, integridad y disponibilidad de la información, teniendo como beneficios la protección de la información, reducción de riesgos, cumplimiento de normativas, mejora de la confianza y optimización de recursos.

g) Gestión de incidentes y acontecimientos relacionados con la seguridad de TI

Comprende la detección, contención, eliminación y recuperación de los incidentes de seguridad de la información, minimizando su impacto en la entidad, con la finalidad de dar cumplimiento a la normativa de seguridad, proteger la información, reducir los riesgos e identificar áreas de mejora de los procesos de seguridad con la implementación de medidas preventivas.

h) Seguridad de la información ligada al personal

Además de una gestión efectiva de los recursos humanos en el ámbito de TI, es esencial implementar programas específicos de concientización, educación y formación en seguridad de la información. Estos programas deben estar debidamente estructurados, aplicarse de forma periódica y adaptarse a las responsabilidades del personal, con especial énfasis en los roles clave relacionados con la gestión de la seguridad en TI. Un enfoque sistemático en la capacitación fortalece la cultura organizacional en materia de seguridad y mejora la preparación frente a posibles amenazas.

2.6.7. Controles de Aplicación

Son controles específicos embebidos en las aplicaciones informáticas para garantizar la validez, integridad, exactitud y disponibilidad de las transacciones y datos durante el ciclo de procesamiento, asimismo, garantizan el cumplimiento de la normativa vigente aplicable. Incluyen controles de entrada, procesamiento, salida, y de seguridad, y son fundamentales para asegurar que las transacciones automatizadas sean confiables, integras y cumplan con los objetivos de la Entidad.

Elementos clave para los controles de aplicación

a) Controles de datos de entrada

La integridad y confiabilidad de los datos en los sistemas de información depende de la implementación de controles adecuados durante su ingreso y procesamiento. Es fundamental contar con validaciones automáticas que aseguren el cumplimiento de campos obligatorios, formatos y rangos de valores, así como mecanismos que eviten la duplicación de registros o datos clave. Además, los usuarios deben tener roles y permisos claramente definidos para garantizar un ingreso controlado de información. Las modificaciones a los datos

deben quedar registradas en bitácoras o logs, y es necesario disponer de procedimientos documentados para la preparación y validación de la información fuente, lo que contribuye a mantener la calidad y trazabilidad de los datos.

b) Controles de procesamiento

El correcto funcionamiento de los sistemas de información requiere que el procesamiento de datos se realice de forma automática, conforme a reglas de negocio documentadas y con resultados consistentes. Para garantizar la integridad y confiabilidad del procesamiento, es esencial implementar controles como totales de verificación, registros en bitácoras de auditoría, alertas automáticas ante errores y mecanismos para el manejo de excepciones en transacciones críticas. Además, deben realizarse revisiones funcionales y técnicas de la lógica implementada en el sistema, así como asegurar que se apliquen controles de integridad a lo largo de todo el ciclo de procesamiento. Estos elementos permiten mantener la precisión, trazabilidad y seguridad de las operaciones.

c) Controles de los datos de salida

La generación de reportes en los sistemas de información debe garantizar la fidelidad, precisión, completitud y oportunidad de los datos procesados. Es fundamental que estos reportes cuenten con mecanismos de revisión y aprobación previos a su distribución, así como controles integrados como sumas de verificación o numeración de páginas. La distribución debe estar debidamente controlada y documentada, y en el caso de reportes que contienen información sensible, deben establecerse restricciones de acceso. Además, deben existir procedimientos para conciliar los datos de entrada y salida, asegurando así la coherencia y confiabilidad de la información presentada.

d) Controles de seguridad de aplicaciones

La gestión de accesos en los sistemas de información es clave para garantizar la seguridad y confidencialidad de los datos. Es esencial contar con perfiles de acceso claramente definidos y documentados, junto con mecanismos de autenticación y autorización que controlen adecuadamente quién accede a qué información. La protección de los datos, tanto en tránsito como en reposo, debe asegurarse mediante cifrado u otras técnicas, complementada por registros de acceso que se monitoreen de forma periódica. Asimismo, la segregación de funciones en operaciones críticas, la autorización formal para cambios de permisos, la detección de incidentes de seguridad y las revisiones periódicas de accesos contribuyen a fortalecer el control y reducir riesgos en el entorno digital.

CAPÍTULO 3

3. PROCESO DE LA AUDITORÍA INFORMÁTICA

Se inicia con la emisión de la orden de trabajo, que contiene el alcance, período examinado, objetivos y recursos establecidos para su ejecución; comprende las fases de planificación, ejecución y emisión del informe, en cada una de ellas se dará cumplimiento al debido proceso.

Para la realización de la auditoría informática se considera que el tiempo asignado se distribuya de la siguiente manera:

Fase	Tiempo asignado (%)
Planificación	40
Ejecución	40
Borrador de informe y conferencia final	20
Total	**100**

A continuación, se describe cada una de estas fases:

3.1. FASE DE PLANIFICACIÓN

La planificación es una fase esencial del proceso de auditoría informática. Su propósito es orientar los esfuerzos del equipo auditor hacia el análisis de los componentes críticos de TI de la entidad auditada, asegurando el uso eficiente de los recursos bajo un enfoque basado en riesgos, alineado con los objetivos institucionales y los marcos normativos aplicables, considerando el nivel de madurez de TI de la entidad y la disponibilidad de los recursos para cumplir con su planificación.

Para determinar el nivel de madurez de TI en una entidad se aplicarán los procedimientos establecidos en la Guía Técnica para la Realización de Auditorías Informáticas.

Esta etapa proporciona los insumos necesarios para definir el alcance de la auditoría, los objetivos específicos, la metodología a aplicar, la asignación de recursos técnicos y humanos, así como el cronograma de ejecución.

En el contexto actual, caracterizado por una alta dependencia institucional de los sistemas de información para el cumplimiento de funciones sustantivas, de apoyo y de control que permiten asegurar el logro de la misión y objetivos institucionales, una planificación eficaz resulta indispensable, a través de la identificación de vulnerabilidades, deficiencias del control interno y riesgos tecnológicos que podrían comprometer la confidencialidad, integridad, disponibilidad y legalidad de la información institucional.

Como parte de esta fase, se recopila y analiza información sobre el marco normativo de la entidad, organización y funcionamiento de las unidades de TI, los procesos, las políticas de seguridad, los sistemas y aplicativos informáticos y la infraestructura tecnológica utilizada para su operación, los mecanismos de monitoreo y alerta, la gestión de incidentes, así como los procedimientos de seguimiento y evaluación de controles.

3.1.1. Planificación general

La planificación general de la auditoría informática comprende un conjunto de actividades que permiten al auditor conocer a la entidad y determinar los riesgos asociados a los componentes y gestión de TI a ser analizados, para lo cual se podrá considerar los siguientes aspectos:

Conocimiento de la entidad

Comprende el diagnóstico de los procesos de la Entidad auditada mediante:

- El conocimiento del marco normativo de la creación, misión, visión, objetivos estratégicos de la entidad, de las políticas públicas nacionales que orientan la transformación digital del Estado y simplificación de trámites.

  Sobre la base del alcance de la acción de control, la identificación de los procesos gobernantes, sustantivos, adjetivos de asesoría y de apoyo, su marco normativo, los convenios y mecanismos de intercambio de información con fuentes externas.

  Aspectos que permiten al equipo auditor, evaluar el cumplimiento de obligaciones legales y técnicas, identificar posibles riesgos institucionales y establecer criterios objetivos para orientar el alcance y las pruebas de auditoría durante su ejecución.

- Conocimiento del área, proyecto, programa o componente tecnológico a examinar y su naturaleza jurídica, así como, procesos de contratación relacionados con el alcance de la acción de control.

- Recopilación de información sobre las acciones realizadas por la Entidad para el cumplimiento de las recomendaciones de los informes aprobados durante el período de análisis de la auditoría y de los sistemas de la CGE implementados para este propósito.

Los aspectos descritos constituyen insumos para la evaluación del control interno que permite al auditor determinar el enfoque y aplicación de procedimientos durante la ejecución de la auditoría.

Evaluación del control interno y riesgos de TI

La evaluación del control interno y riesgos de TI, comprende:

- Identificar y documentar los procesos claves con la finalidad de determinar la existencia de controles implementados y su funcionamiento.

- Efectuar pruebas de funcionamiento y cumplimiento de los controles, de penetración y/o seguridad de ser el caso, y documentar sus resultados.

- Identificar posibles limitaciones para el análisis de los componentes en la ejecución de la auditoría informática, para lo cual se observarán los criterios sugeridos en la Guía Técnica para la Realización de Auditorías Informáticas.

- Identificar posibles exclusiones para el análisis de los componentes en la ejecución de la auditoría informática, para lo cual se observarán los criterios sugeridos en la Guía Técnica para la Realización de Auditorías Informáticas.

- Elaborar la matriz de evaluación de control interno, que incluya los cuestionarios para la verificación del cumplimiento de la normativa, políticas, procesos y procedimientos emitidas por la entidad, con la identificación y documentación de los medios de verificación, estableciendo criterios y ponderación de evaluación, que permitan determinar el nivel de riesgo de TI y confianza del funcionamiento de los controles.

- Los componentes que presentaron incumplimientos como resultado de la evaluación de control interno, constituyen el insumo para la formulación de la matriz de riesgos, lo que servirá para establecer el enfoque de auditoría, con el propósito de determinar las pruebas de auditoría a aplicar sean estas sustantivas, de cumplimiento o de doble propósito, y la formulación de los puntos de interés, hechos reportables, plan de muestreo y programas de auditoría.

  Entendiéndose como puntos de interés, las áreas, procesos o actividades que, por su naturaleza, importancia o nivel de riesgo, relacionados con el alcance del examen son identificados por el equipo de auditoría para profundizar su análisis durante la ejecución del examen. Ejem.: Asignación de roles y perfiles para el acceso a los sistemas sin documentación de respaldo.

Los hechos reportables, constituyen situaciones, eventos o condiciones que pueden afectar la legalidad, eficiencia, eficacia o economía de la gestión pública y que podrían dar lugar a hallazgos si se confirma con evidencia suficiente, competente y pertinente, redactados de manera sucinta con los atributos de condición, criterio, causa y efecto. Ejem.: Se identificó que 250 usuarios del sistema de rastreo de líneas telefónicas tuvieron acceso a la plataforma con privilegios de administración, sin que exista documentación que respalde la solicitud de acceso efectuada por el responsable del área y autorización del oficial de seguridad de la información; contrario a lo dispuesto en la norma de control interno y EGSI; por cuanto no existió el control en la asignación y revisión periódica de los privilegios en los sistemas informáticos; ocasionando que existan transacciones no autorizadas realizadas por los usuarios en referencia.

- Será parte integrante de la planificación, la descripción del personal requerido, la distribución del trabajo a través de los programas de auditoría, el cronograma de trabajo con los hitos a cumplir y los recursos financieros.

- Se identifica la necesidad de utilizar herramientas técnicas de auditoría asistidas por computador (TAACS), con la finalidad de optimizar el análisis del auditor a grandes volúmenes de información y/o procesos automatizados de acuerdo al alcance de la auditoría.

3.1.2. Control Interno

El control interno en Tecnologías de la Información (TI) es un proceso continuo mediante el cual la entidad implementa medidas, políticas y procedimientos destinados a verificar que las actividades relacionadas con los sistemas tecnológicos sean coherentes con las políticas, normas y planes previamente aprobados. Su finalidad es asegurar el funcionamiento continuo, seguro y eficiente del sistema de TI.

Los controles internos abarcan la gestión de riesgos, el cumplimiento de procedimientos e instrucciones internas, así como leyes y regulaciones externas aplicables.

Es necesario considerar que cuando los riesgos se materializan, sus impactos pueden recaer directamente en el servicio a la ciudadanía y, por ende, en el cumplimiento de la misión institucional (transparencia, eficiencia, seguridad y provisión ininterrumpida de servicios públicos); la auditoría informática de la CGE, por tanto, debe identificar y evaluar estos riesgos para priorizar los esfuerzos de control y asegurar que la tecnología contribuya al valor público.

El objetivo principal del control interno informático es supervisar, evaluar y fortalecer continuamente tanto los controles generales que establecen un entorno tecnológico seguro y confiable para la gestión de la infraestructura tecnológica, el desarrollo, operación y mantenimiento de los sistemas como los controles de aplicación, que garantizan la integridad, confidencialidad y exactitud de los procesos automatizados en cada sistema o software específico y servicios tecnológicos.

Controles generales

Control	Descripción	Elementos
Organización y operación	Estructura y normas operativas para toda la organización	- Estructura organizacional - Políticas y planes estratégicos de TI - Planes operativos y de contratación - Normas y procedimientos de TI - Procedimiento de operación diarios documentados - Monitoreo y registro de actividades de sistemas (logs) - Gestión de incidentes y problemas
Seguridad Lógica y Física	Seguridad lógica comprende las configuraciones para evitar el acceso a las	- Políticas de seguridad - Identificación de usuarios - Gestión de usuarios

Control	Descripción	Elementos
	personas no autorizadas y la física es la seguridad que dispone el entorno de trabajo donde se encuentra el equipamiento tecnológico	- Seguridad Física de servidores y equipos críticos - Programas de protección frente a malware (antivirus)
Proceso de desarrollo y mantenimiento	Normas, procedimientos o estándares de desarrollo	- Procedimientos para gestionar los cambios - Designación de personal autorizado para gestión de cambios - Procedimientos y protocolos específicos para cambios emergentes - Ambientes de desarrollo, pruebas y productivos, que cumplan la segregación de funciones - Procedimientos formales (metodologías) para desarrollar, modificar y aprobar software
Controles de adquisición de hardware y software	Relación con el exterior de la organización de TI	- Procedimientos de adquisición de aplicaciones e infraestructura de TI - Gestión de incidencias con proveedores externos - Licenciamiento - Procedimientos de monitoreo y supervisión de los procesos productivos (hardware, servicios de comunicación, aplicativos, bases de datos) - Control de la ejecución de procesos automáticos
Respaldo y Recuperación	Mecanismos implementados para proteger la información y garantizar su disponibilidad en el caso de fallas, errores, pérdidas de datos o desastres	- Políticas de copias de seguridad (frecuencia, almacenamiento seguro) - Verificación periódica de la restauración de respaldos - Planes de recuperación ante desastres (DRP) - Plan de continuidad del negocio (BCP)

Controles de aplicación

Permiten que los sistemas de información sean efectivos y eficientes, así como la información sea íntegra, confidencial, se encuentre disponible, cumpla con la regulación normativa y sea confiable.

Control	Descripción	Elementos
Entrada de datos	Garantiza la integridad de la información	- Procesamiento o transformación, validación y corrección de datos.
Tratamiento de datos	Evita que procesos no autorizados modifiquen datos	- Procesamiento de transacciones completo, adecuado y autorizado
Salida de datos	Permiten identificar las operaciones realizadas con los datos para obtener las salidas	- Informes de errores de la aplicación (incidentes)
Logs	Trazabilidad de las transacciones realizadas en el sistema de información	- Pistas de auditoría para el análisis de hechos anómalos en el funcionamiento de la aplicación

La implementación de los controles generales y de aplicación, garantiza a la entidad la integridad, disponibilidad y confidencialidad de la información, con el propósito de prevenir, detectar y corregir irregularidades, errores e inconsistencias que puedan afectar el desempeño operativo y el cumplimiento de los objetivos institucionales. En consecuencia, se busca asegurar la continuidad de los servicios tecnológicos, y fortalecer la gestión institucional para el logro de los objetivos institucionales, a través de la prevención, detección y corrección de eventos no deseados.

Gestión de riesgos

Comprende la identificación, análisis y evaluación de los riesgos asociados a las aplicaciones, la infraestructura y los servicios de tecnologías de la información, así como a la información generada, procesada y almacenada por estos medios. Incluye además una gestión continua, que contempla la revisión periódica de los riesgos detectados y el monitoreo de la efectividad de las estrategias de mitigación implementadas.

Mecanismos de cumplimiento normativo

Se realiza con la definición de estrategias para la revisión permanente de la aplicación de las políticas, normas y procedimientos asociados; basadas en la comunicación, concientización de los servidores y personal relacionado en las actividades de las áreas de tecnologías de la información y comunicación, usuarios de servicios, proveedores de bienes y servicios tecnológicos.

Otros mecanismos de apoyo al cumplimiento, constituyen el grupo de aseguramiento de la calidad, personal de seguridad de la información y herramientas automatizadas, parametrizadas con los criterios establecidos en las políticas de seguridad.

Una evaluación independiente, instrumentada mediante auditorías (o revisiones) internas o externas, puede brindar información oportuna acerca del cumplimiento del área de TI con las políticas, normas, procedimientos y objetivos generales de la entidad.

3.1.2.1. Evaluación al sistema de control interno

La evaluación de control interno en auditorías informáticas consiste en el análisis de la estructura, diseño y efectividad de los controles implementados en los sistemas informáticos e infraestructura tecnológica de una entidad, con el propósito de determinar si estos son adecuados y eficaces para garantizar la

confidencialidad, integridad, disponibilidad y legalidad de la información institucional.

Este análisis considera tanto los controles generales de TI como implementación de controles de aplicación a base de la normativa y procesos establecidos, configuraciones en los equipos e infraestructura, gestión de accesos, seguridad física y lógica, continuidad del servicio, administración de cambios y control de operaciones.

La evaluación se realiza bajo un enfoque basado en riesgos, con la finalidad de obtener los niveles de riesgo y confianza, mediante la aplicación de técnicas como entrevistas y cuestionarios, considerando el cumplimiento de políticas internas, marcos normativos gubernamentales, institucionales, disposiciones legales aplicables al sector público y marcos de referencia que constituyen mejores prácticas para la gestión de TI como son COBIT, ITL, ISO/IEC 27001, y principios del informe COSO, entre otros.

La estructura de la matriz de evaluación de control interno será la siguiente:

No.	Componente	Control Existente	PT	Respuesta (SI = 1/NO = 0)	CT (1/ 0)	Medio de verificación	Normativa	Observaciones

Los criterios para el desarrollo de la matriz de evaluación del control interno serán los siguientes:

a) Identificación de los componentes para el análisis de la auditoría conforme al alcance de la orden de trabajo.

b) Control existente, corresponde al detalle de los controles identificados por el auditor en la normativa, procesos y procedimientos resultado de las entrevistas y relevamiento de la documentación.

c) En la columna PT (Total preguntas) corresponde a la sumatoria total de los controles evaluados.

d) Los criterios para la evaluación de los controles se presentan a continuación, y de acuerdo a su respuesta su equivalencia cuantitativa, la que se calculará de manera automática.

Criterios de evaluación	Respuesta (SI / NO) (*)	Ponderación (CT)
Control existente	NO	0
Funciona Control existente	SI	1
Control no relevante o modificación de condiciones durante el alcance de la auditoría. Ejem.: Cambio normativo	No aplicable	-

(*) En caso que la respuesta sea **SI** la ponderación es **1**, caso contrario es **0**.

CT: corresponde a la sumatoria de los controles evaluados para cada uno de los componentes.

e) Medios de verificación, permite al auditor informático describir la documentación que respalda la calificación asignada en la evaluación del control interno.

f) Normativa, permite al auditor informático identificar la base legal, política o procedimiento técnico que respalda la existencia o necesidad del control evaluado.

g) Observaciones, permite al auditor informático documentar información cualitativa que complementa la valoración asignada al control y es clave para interpretar correctamente los resultados y tomar las decisiones informadas.

h) Al resultado de la evaluación de los controles por cada componente, se aplican los criterios de ponderación con el propósito de obtener los niveles de riesgo de control y de confianza presentes en cada caso.

Componente	Nivel			
	Riesgo		Confianza	
	CT/PT (%)	Nivel (Bajo, Medio (moderado) y Alto)	1-(CT/PT) (%)	Nivel (Bajo, Medio (moderado) y Alto)
Gobernanza y Gestión de TI				
Desarrollo y Adquisición de TI				

Los posibles niveles a obtener se establecen como: Bajo, Medio (moderado) y Alto, de acuerdo a las siguientes escalas de ponderación:

Nivel	Escala
Alto	>=75%
Medio (moderado)	>50% y <75%
Bajo	<=50%

Siendo la ponderación obtenida, la relación entre la sumatoria de los controles evaluados para cada uno de los componentes (CT) y la sumatoria total de los controles evaluados.

Los resultados de esta evaluación permiten al auditor identificar debilidades, riesgos de seguridad informática y oportunidades de mejora que permitan asegurar la disponibilidad y continuidad de la prestación de los servicios tecnológicos que coadyubarán el cumplimiento de los objetivos institucionales y la eficacia de los procesos apoyados por las soluciones tecnológicas.

Anexo 3. - Cuestionario de evaluación de Control Interno al componente "Desarrollo de sistemas"

Anexo 4. - Matriz de evaluación y calificación del riesgo al componente "Desarrollo de sistemas"

Componentes a evaluar

Los controles a evaluar para los componentes definidos, considerando el alcance de la auditoría y el nivel de madurez de la entidad auditada sin perjuicio de los controles que el auditor pueda identificar en el desarrollo de la auditoría y del avance tecnológico, se detallan en la "Guía Técnica para la realización de Auditorías Informáticas".

Gobernanza y Gestión de TI

a) Estrategia y planificación de TI

- La planificación mediante la formulación de planes estratégicos, operativos y de adquisiciones aprobados y vigentes.
- El PETI alineado con el plan estratégico institucional, planes y políticas de gobierno.

b) Estructuras, normas, políticas y procesos institucionales

- Definición de una estructura organizacional con las áreas necesarias para su funcionamiento.
- Posicionamiento a nivel directivo e independencia de la Unidad de TI a nivel institucional; y con el rol de asesoramiento a la alta dirección.
- Políticas, normas y procedimientos específicos para la gestión de tecnologías de la información, alineadas a los objetivos institucionales, y que se encuentren documentados y aprobados.
- Políticas y disposiciones comunicadas y accesibles para aplicación interna y externa.
- Atribuciones, responsabilidades y asignación de actividades comunicadas de manera formal, con una adecuada segregación de funciones

especialmente en procesos críticos como la gestión de accesos, administración de infraestructura, seguridad de la información y adquisiciones tecnológicas.
- Definición y aplicación del código de ética de la Entidad que incluya principios de TI.
- De acuerdo al nivel de madurez de la entidad, la conformación de un Comité de Gobernanza de TI responsable de revisar, aprobar y asignar fondos para inversiones en TI, así como asegurar que las decisiones estratégicas sobre tecnología estén alineadas con los objetivos institucionales.
- Designación de un oficial de Seguridad de la Información institucional, de acuerdo al nivel de madurez de la entidad y cumplimiento de las funciones asignadas.

c) *Gestión de los recursos humanos de TI*

- Políticas de talento humano relacionadas con TI, su aprobación y actualización.
- Definición de perfiles y roles para el personal de las áreas de TI y planes de capacitación de los mismos.

d) *Gestión de riesgos de TI*

- Plan de riesgos de TI documentado y aprobado, con la identificación y tratamiento de riesgos.

Desarrollo y Adquisición de TI

a) *Estudio de factibilidad*

- La viabilidad técnica, económica, legal, operativa y de tiempo.
- Requerimientos formalizados.

- Informe de análisis de mercado conforme a la solución tecnológica requerida.
- Adecuación del estudio de factibilidad con la realidad institucional.
- Análisis de sostenibilidad en el tiempo y alineación con los objetivos estratégicos de la entidad.
- Informe con las alternativas y soluciones propuestas con las recomendaciones para la toma de decisiones.
- Plan de riesgos para el requerimiento de la solución tecnológica.

b) *Desarrollo y gestión de requisitos*

- Documentación del establecimiento de la necesidad, formalizada por las partes interesadas.
- Documentación del levantamiento de los requerimientos, con la clasificación y priorización de requisitos, incluyendo los de seguridad de la información.
- Informe de evaluación del impacto de los requerimientos sobre la arquitectura, procesos y normativa.

c) *Gestión y control de proyectos*

- Metodología aprobada para la gestión de proyectos de TI.
- Estructura del proyecto que al menos cuente con un director, un responsable de análisis y control de riesgos, personal de aseguramiento de la calidad, gestión de la configuración y personal para realizar las pruebas.
- Designación de los responsables y roles establecidos para la gestión del proyecto, como mínimo un gestor o administrador, quien será el nexo entre los promotores y el equipo de desarrollo (áreas y personal técnico de TI o a su vez proveedor de la solución tecnológica).
- Informes de avance y cumplimiento de hitos y productos de acuerdo al cronograma establecido y de cierre de proyecto.
- Documentación del expediente del proyecto, cronológica y completa.

- Actas de reunión formalizadas, con la aprobación de las partes interesadas y/o equipo técnico.

Para el caso de desarrollo de software, las organizaciones pueden considerar diferentes metodologías del *"Ciclo de Vida del Desarrollo del Software"*, como por ejemplo el modelo de cascada, el modelo en espiral, modelos ágiles y desarrollo iterativo, entre otras, considerando la que mejor se adapte a la consecución de los objetivos institucionales y de la tecnología de la información y comunicación disponible, para lo cual se verificará:

- Metodología aprobada, que contemple todas las etapas del ciclo de vida del desarrollo, la identificación de hitos y productos entregables en cada uno de ellos, responsables de su ejecución, revisión y aprobación.
- Documentación formalizada del desarrollo de la solución de TI generada en cada una de las fases.

d) *Diseño/Desarrollo*

Diseño de soluciones de software:

- Arquitectura del desarrollo del sistema o aplicativo, aprobada.
- Análisis y documentación de respaldo de la definición de los componentes de software y hardware requeridos para la solución tecnológica propuesta.

En caso de que la institución decida la adquisición de las soluciones tecnológicas, se verificará:

- Documentación de estudios y diseños completos con el análisis técnico de la determinación de las especificaciones técnicas de acuerdo a las condiciones establecidas en la normativa de contratación aplicable tanto para bienes y/o servicios según corresponda.

- Estudio de mercado que incluya cotizaciones de proveedores autorizados y con experiencia en la provisión de servicios de TI en desarrollo de soluciones.

Desarrollo de soluciones de software:

Para el caso del desarrollo realizado internamente o contratado, deberá cumplir con los lineamientos establecidos en las metodologías, para lo cual se verificarán los siguientes controles:

- Requisitos técnicos que incluyan los procedimientos y estándares definidos por la entidad para el desarrollo de la solución a nivel de codificación o programación y diseño de base de datos, a fin de asegurar que el producto final esté alineado a los estándares de desarrollo de la entidad.
- Requisitos técnicos y compromisos contractuales que incluyan la capacitación y transferencia de conocimientos al personal técnico de la Unidad de TI y usuarios funcionales, a fin de facilitar la administración y gestión de cambios de la solución posterior a la entrega definitiva por parte del proveedor y finalización de la garantía y soporte contratado.
- Compromisos contractuales para la entrega del código fuente actualizado con la última versión de la solución implementada en el ambiente de producción, a fin de garantizar los cambios o mejoras que se requieran, y trámite para la propiedad intelectual de los sistemas o aplicativos.

e) *Aseguramiento de la calidad y pruebas*

- Plan de pruebas aprobado que contenga el alcance, recursos, cronograma y tipos de prueba a ejecutar, realizado en función de los requerimientos funcionales y técnicos definidos, procesos y normativa relacionada.
- Baterías o casos de prueba definidos.

- Documentación de las pruebas de aceptación y sus resultados formalizados por las partes interesadas correspondientes y personas que intervinieron durante el proceso de pruebas delegados de las áreas funcional y técnica.
- Definición de condiciones para la realización de pruebas de rendimiento (carga, estrés y concurrencia) y de seguridad.
- Controles de criterios de aceptación de los sistemas.

f) *Gestión de la configuración*

- Plan de gestión de la configuración, actualizado y formalizado.
- Inventario de activos de configuración, de los componentes de TI, como: equipos servidores (sistemas operativos, aplicaciones y bases de datos), computadores y dispositivos para el usuario final, software, redes de computación, equipos de seguridad, entre otros recursos.
- Registro de los cambios en las configuraciones, con el detalle del sistema y componentes de TI relacionados con el cambio.
- Base de conocimiento de los cambios en la configuración, que incluya la identificación de cada componente de TI, los atributos, dependencias y cambios efectuados, que permita dimensionar la afectación y sus riegos asociados.
- Informes de auditoría de la configuración, aprobados.

g) *Adquisición de Infraestructura tecnológica*

- Planes de adquisición, aprobados y alineados con la estrategia de TI y el presupuesto aprobado.
- Inventario actualizado de hardware, software y licenciamiento.
- Justificación de la necesidad de la adquisición.
- Establecimiento de requerimientos técnicos.
- Procedimiento aplicado para la baja de bienes.
- Control de las cláusulas contractuales establecidas en los contratos para adquisición de bienes tecnológicos.
- Documentación de la distribución y asignación, de los bienes tecnológicos.

Operaciones de TI

a) *Gestión de la capacidad*

- Análisis periódico de la capacidad y desempeño de los activos y servicios de acuerdo a su criticidad.
- Análisis actualizado de la demanda actual y proyectada, de los servicios y activos de TI.
- Reportes de monitoreo y análisis continuo del rendimiento de la infraestructura tecnológica instalada (memoria, procesamiento, almacenamiento y servicios de conectividad, entre otros.).

b) *Gestión de cambios*

- Procedimientos completos, actualizados y aprobados de gestión de cambios.
- Documentación de autorización de los cambios efectuados por las instancias correspondientes, previo a su implementación, y de existir por el Comité de Control de Cambios o la autoridad competente que cumpla esa función.
- Registro actualizado de los cambios efectuados con la justificación, solicitante, fecha, estado, resultado, con la identificación de las instancias de aprobación.
- Documentación de pruebas, supervisión y aceptación de los cambios, previo a su implementación.
- Documentación y justificativos de los cambios no aprobados.

c) *Gestión de incidentes y problemas*

- Procedimientos aprobados y actualizados para la gestión de incidentes y problemas, que incluya criterios de priorización, escalamiento y tiempos de atención.

- Solicitudes de incidentes y problemas, con la bitácora de registros.
- Base de conocimientos de los incidentes y problemas más frecuentes, con las soluciones y tiempos de atención.

d) *Gestión de servicios*

- Catálogo de servicios actualizado, con la descripción de los servicios de TI.
- Verificar que se cuente con registros para la gestión de los servicios considerados en el catálogo.
- Clasificación de los servicios por criticidad, disponibilidad, horarios de atención y prioridades.
- Sistemas o mecanismos de monitoreo para medir los indicadores establecidos en los SLA.
- SLA, OLA y UC definidos, aprobados y gestionados, aplicados al menos para los servicios críticos.
- Reportes de monitoreo, supervisión, revisión y cumplimiento de los SLA, OLA y UC.
- Documentación de acciones correctivas ante incumplimientos de SLA.

e) *Gestión de activos de TI*

- Procedimiento de gestión de activos actualizado, aprobado y aplicado, que contemple todas las etapas del ciclo de vida del activo, adquisición, registro, uso, mantenimiento, monitoreo y disposición final.
- Inventario actualizado y completo de activos de TI (hardware, software, licencias, dispositivos de red, entre otros), en el que conste información clave como tipo de activo, número de serie, ubicación, estado, fechas de adquisición y baja, custodio asignado, proveedor y garantía.
- Procedimientos de eliminación segura de activos con criterios de sostenibilidad.
- Informes de monitoreo permanente del estado, rendimiento y vida útil de los activos, con el fin de prevenir fallos, planificar reemplazos y optimizar costos.

- Procedimiento para la disposición segura de los activos dados de baja, que garantice la eliminación de datos y el cumplimiento de las normativas aplicables.

Externalización

a) Cumplimiento legal y normativo

- Política o procedimiento de externalización de servicios de TI debidamente aprobados por la alta dirección o el comité de gobierno de TI que incluya los aspectos de seguridad de la información, protección de datos, aceptación de bienes y servicios de TI, y propiedad del software.
- Designación de un responsable o delegado de protección de datos, de acuerdo a lo establecido en la normativa aplicable.
- Licenciamiento legal de todos los programas y herramientas.
- Cláusulas contractuales de compromisos de los proveedores tecnológicos, incluyendo las de confidencialidad, SLA, propiedad intelectual, y tratamiento de datos.
- Informes documentados sobre el servicio, brechas de cumplimiento y acciones correctivas.

Gestión de la Continuidad del Negocio

a) Política, planes y organización para la continuidad del negocio

- Política de continuidad del negocio aprobada y comunicada.
- Conformación del Comité y equipo responsable de la continuidad de los sistemas y servicios de TI.
- Plan de continuidad del negocio (BCP), aprobado, con el análisis de impacto a las operaciones críticas, identificación de las acciones, roles y responsabilidades de su ejecución, recursos tecnológicos e instalaciones.
- Plan de recuperación ante desastres actualizado, aprobado y comunicado.

- Plan de respaldo y restauración de datos actualizado, aprobado y comunicado.
- Plan de contingencia actualizado, aprobado y comunicado.
- Documentación de pruebas y simulacros efectuados al plan de continuidad del negocio (BCP) y sus actualizaciones.
- Medidas técnicas y organizativas para reanudar operaciones.
- Capacitación y concientización al personal sobre el plan de continuidad del negocio (BCP).

Seguridad de la Información

a) Evaluación de Riesgos de Seguridad de la Información

- Proceso de evaluación de riesgos de seguridad de la información, formalizado y aplicado.
- Integración de los riesgos de seguridad de la información, ciberseguridad, continuidad del negocio con los riesgos de TI.

b) Política de seguridad de la información

- Política de seguridad de la información, aprobado por la alta dirección o comité respectivo.
- Documentación de la difusión y concientización de la aplicación y cumplimiento de la política de seguridad a todo el personal y terceros.
- Capacitación y concienciación sobre la política de seguridad de la información.
- Documentación con las acciones de supervisión al cumplimiento y aplicación de la política.
- Procedimiento definido y aprobado para identificar, analizar y evaluar riesgos de seguridad de la información.
- Plan de tratamiento de riesgos y amenazas de TI formalizado, con acciones definidas para mitigar o aceptar los riesgos identificados.

c) Organización de la seguridad de TI

- Conformación formal del comité de seguridad de la información u órgano similar, que incluya los roles y responsabilidades.
- De acuerdo al grado de madurez de la entidad, designación del Oficial de Seguridad de la Información.
- Contratos y acciones de personal de los funcionarios, con la inclusión de cláusulas sobre deberes y responsabilidades en seguridad de la información.

d) Gestión de activos de información

- Identificación y clasificación de los activos de TI: equipos, sistemas de información y datos, sus custodios y responsables.
- Atribuciones y responsabilidades para la seguridad y protección de los activos de TI.
- Procedimientos para la baja o devolución de activos cuando estos ya no son necesarios para la entidad garantizando la eliminación segura.

e) Seguridad física y del entorno

- Identificación de las áreas protegidas con la limitación física de su acceso por personal no autorizado.
- Sistemas de control de acceso para restringir el ingreso a áreas seguras y garantizar el ingreso de personal autorizado.
- Seguridad física de la infraestructura de las instalaciones en las que se alberga los activos de información.
- Medidas de detección y prevención, como la instalación de sistemas de alarmas, incendios, con la finalidad de detectar amenazas y prevenir posibles incidentes.
- Control de acceso de visitantes que garanticen la restricción de ingreso a áreas identificadas como críticas, sin autorización.

f) Control de acceso

- Política y procedimientos actualizados y aprobados para el control de acceso lógicos a los sistemas, servicios y controles físicos a equipos de la infraestructura de TI.
- Procedimiento para la conformación y gestión de contraseñas.
- Gestión de incidentes detectados y reportados en el uso de las credenciales de acceso lógicos a los sistemas, servicios y controles físicos a equipos de la infraestructura de TI.
- Registro histórico de transacciones y de accesos.

g) Gestión de incidentes y acontecimientos relacionados con la seguridad de TI

- Procedimiento aprobado para la gestión de incidentes.
- Estructura organizativa con roles y responsabilidades definidos, y canales de comunicación para la atención y respuesta a incidentes.
- Registro actualizado de los incidentes con evidencia documental y trazabilidad que permita su verificación.

h) Seguridad de la información ligada al personal

- Programas de concientización ligados a seguridad de la información, aplicados y probados.
- Elaboración de un plan de formación para los roles claves que gestionan seguridad TI.
- Protocolos de desvinculación, asegurando la revocación de accesos cuando un colaborador se retira o cambia de función.

Controles de Aplicación

a) Controles sobre los Datos de Entrada

- Los datos fuente sean preparados, autorizados e ingresados de forma tal que el sistema acepte únicamente datos válidos, completos y confiables.

b) Controles de Procesamiento

- Los datos mantienen la integridad, validez y confiabilidad durante todo el ciclo de procesamiento.

c) Controles sobre los datos de salida

- Los resultados de las transacciones son completos, precisos y se distribuyen correctamente, además están protegidos contra modificaciones y accesos no autorizados.

d) Controles de seguridad de aplicaciones

- Se asegura la confidencialidad, integridad y disponibilidad de la información procesada por las aplicaciones, se comprenden las interfaces de entrada y salida, así como los mecanismos de almacenamiento de datos.

Tipo de Control	Aspectos a considerar en la auditoría
Entrada de datos	¿Han existido registro de incidencias relacionadas con errores en los datos ingresados reportes con información incompleta, inconsistente o duplicada? ¿Se han establecido procedimientos para la creación de roles y perfiles de usuario para el ingreso, revisión y aprobación de las transacciones?
Procesamiento	¿Se definieron procedimientos o requerimientos que permitan la verificación de cálculos e integridad de la información durante su procesamiento o posterior? ¿Se han establecido mecanismos periódicos de conciliación de totales y las transacciones registradas? ¿Se implementaron mensajes automáticos de error cuando se detectan inconsistencias en la información?
Salida de datos	¿Se implementaron los reportes conforme las necesidades de información y control del proceso examinado? ¿Se identificaron las necesidades y/o requerimientos de información y reportería sin implementar?

Seguridad de la aplicación	¿Están definidos y documentados los perfiles de acceso a la aplicación? ¿Se formularon requerimientos de control para el ingreso, revisión y aprobación de transacciones y su acceso?

3.1.2.2. Seguimiento al cumplimiento de recomendaciones

Se verificará el grado de cumplimiento de las recomendaciones que constan en los informes aprobados por la Contraloría General del Estado emitidos por las unidades de auditoría interna y externa, en el período analizado y relacionados con el alcance de la auditoría informática, considerando las disposiciones de la Ley Orgánica de la Contraloría General del Estado y las emitidas por el Contralor General del Estado. Si las recomendaciones no han sido cumplidas, analizar las causas y comunicar a la administración de la Entidad y a los responsables de su cumplimiento.

Los procedimientos para efectuar el seguimiento de las recomendaciones, se iniciarán en la unidad de control como una actividad planificada en el plan anual de control o como parte de la evaluación a efectuar en un examen a los componentes informáticos, con esta finalidad se recopilarán los informes aprobados en el período de análisis, se verificará en los sistemas informáticos de la CGE el plan de acción y el registro del estado de cumplimiento de las recomendaciones, se analizará y tabulará las recomendaciones en un papel de trabajo.

Como resultado de la evaluación al seguimiento de las recomendaciones, se contemplan los siguientes estados:

- Cumplida, cuando las acciones realizadas por los responsables de la aplicación de las recomendaciones subsanaron las deficiencias formuladas en el informe de auditoría.
- Incumplida, cuando no se han tomado acciones para el cumplimiento de las recomendaciones.

- No aplicables, en los casos de modificación de la estructura orgánica o competencias de las Entidades que hayan dado lugar a la supresión de los procesos, para cuya mejora fueron emitidas las recomendaciones.
- Parcialmente cumplidas, cuando se han efectuado las acciones establecidas en el plan de acción registrado en los sistemas de la CGE, sin haberse subsanado en su totalidad la observación durante el período de alcance de la auditoría.

3.1.3. Riesgos de Auditoría

El auditor informático deberá obtener una comprensión suficiente de los sistemas de información, infraestructura y componentes tecnológicos que administra la entidad, a fin de determinar el enfoque de la auditoría y/o examen especial; se aplicarán criterios técnicos informáticos profesionales a fin de evaluar el riesgo de auditoría que permitan diseñar procedimientos adecuados para asegurar que el riesgo se reduzca a un nivel aceptablemente bajo.

El riesgo de auditoría, es la posibilidad de que la información o actividad sujeta a examen contenga errores o irregularidades significativas en los procesos, sistemas o información evaluada y no sean detectados en la ejecución; estos riesgos pueden ser:

Riesgo inherente

Se refiere a la probabilidad de que existan errores, fallos, vulnerabilidades o irregularidades significativas en los procesos, sistemas, activos y servicios tecnológicos antes de considerar la existencia de controles. Este riesgo está asociado a la naturaleza propia del entorno tecnológico, como su complejidad, nivel de automatización, sensibilidad de la información tratada y exposición a amenazas externas.

Es más alto en sistemas críticos, aplicaciones nuevas o no probadas, entornos con alta dependencia tecnológica, o cuando se requiere un alto grado de juicio humano en el diseño o uso de las herramientas informáticas. Identificar correctamente el riesgo inherente permite al auditor planificar procedimientos más rigurosos y enfocar la revisión en áreas con mayor potencial de impacto.

Riesgo de control

Es la posibilidad de que los controles internos establecidos por la entidad para los procesos, sistemas, activos y servicios tecnológicos no prevengan, detecten o corrijan oportunamente errores, fallos o actividades no autorizadas que puedan afectar la confidencialidad, integridad o disponibilidad de la información, y la continuidad de los servicios.

Entre más eficaces sean los controles de la entidad, menor será el riesgo de control y, por tanto, el auditor podrá establecer una menor cantidad de procedimientos de auditoría; por el contrario, cuando el riesgo de control sea alto, el auditor deberá planificar procedimientos de auditoría que le permitan mitigar esos riesgos.

Riesgo de detección

Es la probabilidad de que los procedimientos aplicados por el auditor informático no identifiquen errores, fallas, omisiones o irregularidades significativas en los procesos, sistemas, activos y servicios tecnológicos evaluados. Este riesgo depende directamente de la calidad, profundidad y eficacia de las pruebas realizadas durante la auditoría.

En la auditoría informática, una vez obtenidos los resultados de la evaluación del control interno, los componentes con los niveles de riesgo de control (medio y alto) conformarán la matriz de riesgos junto con los riesgos inherentes resultado del levantamiento de procesos, entrevistas y revisión de documentación efectuadas por el auditor, así:

Componente	Riesgos		Fundamento (Descripción del riesgo inherente y/o de control)	Controles Claves	Enfoque de Auditoría	
	Inherente (Alto / Moderado / Bajo)	Control (Alto / Moderado / Bajo)			Pruebas de Cumplimiento	Pruebas Sustantivas

Además, es importante considerar el riesgo que puede presentar la entidad, en función de los compontes definidos en el numeral 2.4 de este manual de auditoría informática, los cuales se detallan en el anexo correspondiente.

Componente analizado: son aquellos que evidenciaron la falta de aplicación y funcionamiento de los controles establecidos por la entidad, resultantes de la evaluación de control interno, y los identificados en la evaluación de los riesgos inherentes.

Riesgos y su calificación: corresponde al tipo de riesgo identificado, siendo estos: inherente y de control, en función del componente evaluado, el nivel de riesgo puede ser: alto, moderado y bajo.

Fundamento: en esta columna se describe el riesgo inherente y de control identificados respecto al componente analizado del cual previamente existieron observaciones como resultado de la evaluación de control interno.

Controles clave: en función de los riesgos de control identificados por cada componente, se describen los controles claves de los mismos, puntualizando las estrategias que permitan mitigar estos riesgos.

Enfoque de auditoría: responde a los riesgos identificados, donde se describen y/o detallan los procedimientos producto de los resultados de la evaluación del control interno, con el objetivo de ratificar o no observaciones e inconsistencias que afectan a los componentes evaluados; se definen dos tipos de enfoques a

través de las pruebas realizadas; siendo estas: "*pruebas de cumplimiento*", "*pruebas sustantivas*" o su combinación "*doble propósito*".

(Ver modelo de matriz de Evaluación y Calificación del Riesgo de Auditoría – Caso Práctico, Anexo 4)

3.1.4. Pruebas y Técnicas

Métodos, herramientas y procedimientos de auditoría informática, que permitirán contar con el respaldo del análisis realizado por los auditores, y sustento de las evidencias obtenidas, que serán el insumo para la elaboración de los hallazgos y presentación de los resultados de la auditoría.

3.1.4.1. Pruebas de cumplimiento y sustantivas

Pruebas de cumplimiento

Con estas pruebas se pretende evaluar si los procedimientos y controles establecidos ya sean manuales o automatizados en los sistemas de TI, se están ejecutando de forma efectiva y consistente según lo establecido en leyes, regulaciones y normas tanto internas como externas.

Pruebas sustantivas

Como resultado de la evaluación de los controles de TI, se pueden determinar áreas relevantes para la realización de pruebas específicas, con la finalidad de validar la exactitud, integridad y confiabilidad de los sistemas que procesan y almacenan la información, con la aplicación de técnicas para la consulta, extracción y análisis de datos. Con este propósito, la auditoría debe contar con herramientas para la evaluación de programas, sistemas informáticos, consistencia y validez de datos, mediante herramientas de análisis de datos, revisión directa de sistemas y aplicativos, y comparaciones cruzadas.

Pruebas de doble propósito

Combinan pruebas sustantivas y de cumplimiento que permiten al auditor verificar, en una misma ejecución, la eficacia de los controles automáticos del sistema y al mismo tiempo la precisión o confiabilidad de los datos resultantes o procesados por dicho sistema.

3.1.4.2. Plan de muestreo

Constituye una estrategia para seleccionar y evaluar una muestra representativa de datos, transacciones o controles tecnológicos, con el fin de obtener evidencia suficiente y adecuada sobre el estado del ambiente de control o la confiabilidad de los sistemas de control.

Para el plan de muestreo se pueden plantear las siguientes interrogantes:

¿Qué se va auditar(población)?
¿Cómo se seleccionan los elementos de la muestra (método de muestreo)?
¿Cuántos elementos se van a revisar (tamaño de la muestra)?
¿Por qué el enfoque definido es adecuado (razón de la selección)?

Existen dos clases de muestreo para la auditoría, el muestreo estadístico y no estadístico, el primero se basa en la aplicación de técnicas matemáticas considerando condiciones y parámetros como tamaño de la muestra y su margen de error; y, el segundo tipo de muestreo no aplica técnica matemática alguna, en su lugar su selección está dada por la experiencia del auditor.

Para el propósito de este manual, los métodos de muestreo a aplicar son los siguientes:

- Muestreo aleatorio simple: para asegurar imparcialidad, consiste en extraer una cierta cantidad de la población elegidas al azar, de modo que la probabilidad de extracción de cada muestra posible de tamaño "n" sea igual a la de cualquier otra muestra del mismo tamaño.

- Muestreo estratificado: divide la población por características y selecciona muestras por cada grupo.

Para los métodos indicados con la finalidad de determinar el tamaño de la muestra para análisis, se aplicará la siguiente fórmula:

$$n = \frac{N \cdot Z^2 \cdot p \cdot (1-p)}{(E^2 \cdot (N-1)) + (Z^2 \cdot p \cdot (1-p))}$$

Donde:

n: tamaño de la muestra
N: tamaño de la población
Z: nivel de confianza
p: proporción esperada de error
E: margen de error tolerado

3.1.5. Documento de planificación

El resultado de las actividades de esta fase de la auditoría, se presentan en el documento de planificación el cual será entregado a la unidad de control para su revisión y aprobación.

Anexo 5. - Formato Documento de Planificación (Documento de Planificación General)

Anexo 6. - Programa de Auditoría Informática.

3.2. EJECUCIÓN DE LA AUDITORÍA

La fase de ejecución, es crucial en el proceso de la auditoría, es donde se desarrollan las actividades planificadas en los programas de trabajo se aplican pruebas a fin de recopilar evidencia suficiente, competente y pertinente que respalde los hallazgos de la auditoría.

En esta etapa también se debe mantener comunicación constante con las personas relacionadas con el alcance de la auditoría, la calidad del trabajo en esta fase se determinará la utilidad y credibilidad del informe final.

3.2.1. Consideraciones previas en la ejecución de la Auditoría de TI

Para el desarrollo de la fase de ejecución de la auditoría informática, se empleará el 40% del tiempo asignado para su realización, distribuido en el 30% para la aplicación de las pruebas de auditoría, desarrollo de hallazgos y el 10% restante para la comunicación de resultados.

Se garantizará el cumplimiento del debido proceso a través de las notificaciones y comunicación de resultados a los funcionarios de la Entidad auditada y demás personas relacionadas.

Así también, para el inicio de esta fase se deberá contar con la planificación general de la auditoría aprobada y con la recepción formal de los programas de auditoría por parte de los integrantes del equipo.

Para efectuar los procedimientos establecidos en esta etapa se deberán realizar pruebas de cumplimiento y/o pruebas sustantivas según la estrategia y el enfoque definido.

El equipo de auditoría debe disponer de los recursos necesarios que le permitan realizar sus actividades conforme lo programado y de manera eficiente.

Resultado de la coordinación efectuada con la entidad a auditar, se contará con los permisos de acceso a los componentes tecnológicos motivo de análisis y designación del personal con el que se efectuarán las pruebas y suscribirán la documentación con los resultados de las verificaciones efectuadas.

3.2.2. Pruebas de auditoría de TI.

Para efectuar los procedimientos establecidos en esta etapa se deberán realizar pruebas de cumplimiento, pruebas sustantivas o de doble propósito según los resultados de la planificación de la auditoría, a través de las cuales se espera obtener los elementos de juicio pertinentes para detectar, confirmar o delimitar las posibles incidencias o consecuencias que se pueden presentar en la entidad, por la ausencia o incumplimiento de procedimientos básicos y fundamentales para el correcto funcionamiento del componente auditado.

Al planificar las pruebas de auditoría, el profesional debe considerar al menos tres variables principales:

- ¿Qué tipo de pruebas? (definir la naturaleza de las pruebas).
- ¿Cómo probar? (métodos y procedimientos que permitan realizar la prueba).
- ¿Cuánto probar? (selección de la muestra adecuada de la prueba).

En síntesis, implica definir la naturaleza (qué tipo de pruebas efectuar), el alcance (cuántas pruebas efectuar) y el tiempo asignado (cuándo efectuar las pruebas), se verifican y documentan los resultados, se identifican las desviaciones que servirán de insumos para el desarrollo de los hallazgos y personas relacionadas.

Para la realización de las pruebas de auditoría se debe elaborar un plan detallado de pruebas, indicando el componente, control, tipo de evidencia a

ser examinada, los responsables del equipo de auditoría y de la entidad auditada, y las fechas de inicio y finalización. Se debe contar con papeles de trabajo y documentación formal que respalden los resultados obtenidos de la aplicación de las pruebas.

Anexo 7. - Formato Plan de Pruebas de Auditoría Informática

En este manual, se pone a consideración las pruebas sugeridas por cada uno de los componentes definidos en el apartado 2.4, según "**Anexo 8**. - Pruebas para la ejecución de la Auditoría Informática", que se efectuarán de acuerdo al alcance de la auditoría y el nivel de madurez de la entidad, las que se complementarán con los elementos e instrucciones establecidas en la "Guía Técnica para la realización de Auditorías Informáticas", sin perjuicio de las pruebas que el auditor considere aplicar en la ejecución de la auditoría.

Gobernanza y Gestión de TI

Evaluar la estrategia y planificación del área, verificando la existencia de un portafolio de proyectos priorizado, indicadores de desempeño, participación del Comité de Gobernanza de TI, modelo organizativo claro, aplicación del código de ética y seguimiento a recomendaciones. Así como las estructuras, normas, políticas y procesos organizacionales, asegurando que la unidad de TI funcione según la estructura aprobada, cuente con procesos documentados, controlados y alineados a la planificación institucional, y se apliquen mecanismos de mejora continua. Finalmente, es fundamental auditar la gestión de riesgos de TI, comprobando la identificación, tratamiento y monitoreo de riesgos, así como la comunicación de los resultados al Comité respectivo para la toma de decisiones y aprobación de requerimientos, y la aplicación de un plan de acción alineado con una matriz de riesgos institucional.

Desarrollo y Adquisición de TI

Evaluar el estudio de factibilidad de soluciones tecnológicas, verificando aspectos legales, técnicos, de seguridad, análisis costo-beneficio y riesgos. En el

desarrollo y gestión de requisitos, asegurar que existan documentación completa, cumplimiento de requerimientos funcionales y normativos, participación de las partes interesadas, interoperabilidad, soporte y mantenimiento. En la gestión y control de proyectos, es clave contar con planes aprobados, monitoreo del cronograma, gestión de cambios y cierre formal del proyecto. Para el diseño y desarrollo, verificar la definición adecuada de arquitectura, componentes técnicos y cumplimiento de estándares en la construcción del software, así como la capacitación a usuarios y técnicos. El aseguramiento de la calidad implica revisar que se hayan ejecutado planes de pruebas completos, con documentación de resultados, casos específicos y resolución de problemas. En cuanto a la gestión de configuración, validar la trazabilidad de los cambios, registros actualizados y procedimientos de configuración y versiones. Finalmente, en la adquisición de infraestructura, asegurar que los procesos estén sustentados técnicamente, cumplan normativa vigente, garanticen la compatibilidad e integración con sistemas existentes, y que los bienes estén registrados, documentados y respaldados contractualmente.

Operaciones de TI

El componente de Operaciones de TI se enfoca en evaluar la eficiencia y control de los procesos operativos de tecnología. Incluye la revisión de la gestión de la capacidad, asegurando que los recursos tecnológicos satisfagan la demanda actual y futura; la gestión de cambios, para verificar que existan procedimientos formales que minimicen riesgos y aseguren la trazabilidad de las modificaciones; y la gestión del personal de TI, evaluando la asignación de funciones, competencias y cumplimiento de normativas laborales y éticas. También se analiza la gestión de incidentes y problemas, para confirmar la existencia de mecanismos efectivos de registro, atención y solución oportuna. La gestión de niveles de servicio revisa la existencia y cumplimiento de acuerdos (SLAs) con usuarios y proveedores, y la gestión de activos a través del control del inventario tecnológico, su uso adecuado y mantenimiento actualizado.

Externalización

Evaluar que la entidad gestione adecuadamente los servicios tecnológicos contratados a terceros. Esto implica verificar la existencia de un análisis previo que justifique la externalización, la formalización de contratos con cláusulas claras sobre niveles de servicio, seguridad, confidencialidad y cumplimiento normativo. También revisar que haya mecanismos de supervisión y evaluación del desempeño de los proveedores y control de vulnerabilidades, así como evidencia de seguimiento, mitigación de riesgos y aplicación de medidas correctivas en caso de incumplimientos. Además, es importante comprobar que la externalización no comprometa la continuidad operativa, ni la integridad y confidencialidad de la información.

Gestión de la Continuidad del Negocio

Realizar pruebas para verificar que la entidad cuente con un plan de continuidad operativa (BCP) y un plan de recuperación ante desastres (DRP) formalmente aprobados, actualizados y alineados con los riesgos identificados. Comprobar la existencia de análisis de impacto al negocio (BIA), así como de estrategias documentadas para la recuperación de sistemas críticos. Además, es necesario revisar si se han realizado pruebas periódicas de simulación o validación de dichos planes, con resultados documentados y acciones de mejora. También confirmar que las responsabilidades estén claramente asignadas, que el personal clave haya sido capacitado y que exista un procedimiento definido para la activación de los planes ante eventos disruptivos.

Seguridad de la Información

Evaluar los mecanismos implementados para proteger la confidencialidad, integridad y disponibilidad de la información institucional. Esto incluye verificar la existencia y aplicación de una política de seguridad formal, la definición clara de roles y responsabilidades en la organización de la seguridad de TI, y el control

adecuado sobre los activos de información. También se debe revisar la efectividad de las medidas de seguridad física y del entorno, los controles implementados para el acceso lógico y físico a los sistemas, y los procedimientos establecidos para la gestión de incidentes de seguridad, incluyendo su registro, análisis, respuesta y mejora continua.

Controles de Aplicación

El componente de Controles de Aplicación se enfoca en evaluar la confiabilidad, integridad y seguridad de las funciones automatizadas dentro de los sistemas. Las pruebas deben verificar la existencia de controles sobre los datos de entrada, asegurando su validez, integridad y autorización antes del procesamiento; controles de procesamiento, que garanticen la correcta ejecución de las operaciones conforme a las reglas del negocio; y controles sobre los datos de salida, asegurando la exactitud, confidencialidad y distribución adecuada de la información generada. Además, se deben revisar los controles de seguridad de las aplicaciones, incluyendo restricciones de acceso, trazabilidad de acciones, y medidas que prevengan modificaciones no autorizadas al código o a los datos procesados.

3.2.3. Hallazgos de Auditoría

El término hallazgo se refiere a deficiencias o inconsistencias en el control interno detectadas por el auditor y que, a su juicio, merecen ser comunicados a los funcionarios de la entidad auditada y a otras personas interesadas, ya que representan deficiencias importantes que podrían afectar en forma negativa, su capacidad para registrar, procesar, resumir y reportar información confiable y consistente, en relación con las aseveraciones efectuadas por la administración. Los hallazgos constituyen los comentarios del informe de auditoría.

Anexo 9. - Hoja de Hallazgo

3.2.4. Elementos del Hallazgo de Auditoría

Desarrollar en forma completa todos los elementos del hallazgo en una auditoría, no siempre podría ser posible. Por lo tanto, el auditor debe utilizar su buen juicio y criterio profesional para decidir cómo informar determinada debilidad importante identificada en el control interno. La extensión mínima de cada hallazgo o comentario de auditoría dependerá de cómo éste debe ser informado, aunque por lo menos, el auditor **debe** identificar los siguientes elementos:

- **Condición:** Se refiere a la situación actual encontrada por el auditor al examinar un área, actividad, función u operación, entendida como "**lo que es".**
- **Criterio:** Comprende la concepción de "**lo que debe ser ",** con lo cual el auditor mide la condición del hecho o situación, establece las inobservancias o incumplimientos de la base legal y normativa de rige al hecho.
- **Causa:** Es la razón básica (o las razones) por lo cual ocurrió la condición, o también el motivo del incumplimiento del criterio de la norma. Su identificación requiere de la habilidad y el buen juicio del auditor y, es indispensable para el desarrollo de una recomendación constructiva que prevenga la recurrencia de la condición.
- **Efecto:** Es el resultado adverso o potencial de la condición encontrada, generalmente representa la pérdida en términos monetarios originados por el incumplimiento para el logro de la meta, fines y objetivos institucionales.

3.2.5. Evidencia de Auditoría

En auditoría informática, la evidencia se refiere a cualquier información o prueba que respalde o refute una afirmación o hecho en una auditoría.

La evidencia de auditoría puede incluir:

- Las observaciones del auditor de TI (presentadas a la gerencia)
- Notas tomadas de las entrevistas
- Resultados de confirmaciones independientes obtenidas por el auditor de TI de diferentes partes interesadas
- Material extraído de correspondencia, correos electrónicos y documentación interna o contratos con terceros externos
- Los resultados de los procedimientos de pruebas de auditoría

Las evidencias de auditoría constituyen los elementos de prueba que obtiene el auditor sobre los hechos que examina, y son el respaldo de la auditoría que sustenta el contenido del informe.

Ejemplos de evidencia:

- Registros de acceso: Permiten verificar quién accedió a qué sistemas o datos y cuándo.
- Documentos de políticas y procedimientos: Demuestran que la institución tiene políticas y procedimientos de seguridad informática definidos.
- Logs de sistema: Registran los eventos que ocurren en los sistemas informáticos, incluyendo fallos, errores y operaciones realizadas.
- Documentos de respaldo y recuperación: Proporcionan evidencia de que la institución tiene planes de respaldo y recuperación de datos.
- Documentos de proveedores: Se utilizan para verificar la información proporcionada por los proveedores de servicios informáticos.
- Contratos y acuerdos: Demuestran los acuerdos y compromisos de la institución en materia de seguridad informática.
- Informes de auditoría anteriores: Permiten evaluar la efectividad de las medidas de seguridad tomadas y la evolución de los riesgos.

Las evidencias se clasifican en:

- **Física:** Que se obtiene mediante inspección u observación directa de las actividades, bienes, documentos y registros. La evidencia de esta naturaleza puede incluir hardware, software, dispositivos de almacenamiento, etc.
- **Documental:** Consiste en la información elaborada, como la contenida en cartas, contratos, informes, correos electrónicos y documentos de la administración relacionada con su desempeño (internos), y aquellos que se originan fuera de la entidad (externos).
- **Analítica:** Se obtiene al analizar o verificar la información, el juicio profesional del auditor acumulado a través de la experiencia que orienta y facilita el análisis, son los resultados obtenidos de las pruebas sustantivas.

Técnicas para la recopilación de evidencia

- **Revisión de las estructuras organizacionales de TI**: una estructura organizacional que provee una adecuada separación o segregación de funciones es un control general clave en un ambiente de sistemas de información
- **Revisión de políticas y procedimientos de TI:** un auditor de TI debe revisar si existen políticas y procedimientos apropiados, determinar si el personal las entiende y garantizar que las aplican.
- **Revisión de los estándares de TI:** el auditor de TI debería entender los estándares vigentes existentes dentro de la organización.
- **Revisión de la documentación de TI:** el auditor de TI debe buscar documentación de TI, que puede incluir: documentos de inicio de desarrollo de sistemas, documentación suministrada por proveedores externos, SLA con proveedores externos, manuales, planes, reportes.
- **Entrevistas al personal apropiado:** las entrevistas deben ser organizadas de antemano con objetivos claramente comunicados.
- **Recorridos (walk-throughs):** La prueba de recorrido es una técnica de auditoría para confirmar el entendimiento de los controles

Atributos de la Evidencia:

Para que sea una evidencia de auditoría, se requiere la unión de dos elementos: evidencia suficiente (característica cuantitativa) y evidencia comprobatoria o competente (característica cualitativa), que proporcionan al auditor la convicción necesaria que le permita tener una base objetiva de la auditoría.

Los atributos de la evidencia son:

- **Suficiencia. -** Se refiere al volumen o cantidad de la evidencia, tanto en sus cualidades de pertinencia y competencia. El concepto de suficiencia reconoce que el auditor no puede reducir el riesgo de auditoría a cero y el "SAS-31- Evidencias de Auditoría" pone énfasis en que la acumulación de evidencias debe ser más persuasiva que convincente.

- **Competencia. -** Para que la evidencia sea competente, debe ser válida y confiable. A fin de evaluar la competencia de la evidencia, el auditor debe considerar si existen razones para dudar de su validez o su integridad. Si bien toda la evidencia apoya al auditor de TI en el desarrollo de las conclusiones de la auditoría, ciertos tipos de evidencia son más confiables que otros:

    - La evidencia obtenida de fuentes externas es más confiable que la obtenida dentro de la institución.
    - El auditor de TI debería siempre considerar las credenciales y responsabilidades funcionales de las personas que suministran la información o evidencia independientemente de si estas personas son internas o externas.
    - La evidencia objetiva es más confiable que la evidencia que requiere opinión o interpretación considerable.
    - El auditor de TI debería considerar el tiempo durante el cual la información existe o está disponible al determinar la naturaleza, el tiempo y la extensión de las pruebas de cumplimiento y si fuera aplicable las pruebas sustantivas.

- **Pertinencia o Relevancia.-** Es aquella evidencia significativa relacionada con el hallazgo específico.

En conclusión, los hallazgos de auditoría deben sustentarse en evidencia, de modo tal que la cantidad y calidad de la evidencia obtenida tengan relevancia. Esto significa que un auditor de TI debe considerar y evaluar continuamente la evidencia que planea obtener, o que ha obtenido, en lo relativo a su suficiencia, competencia y pertinencia. Los auditores pueden evaluar si la evidencia es relevante y confiable al considerar, entre otras cosas, la naturaleza de la fuente y su reputación, los controles operados por la entidad auditada, la presencia de evidencia contradictoria o confirmatoria, y los métodos, modelos y supuestos a los que se recurrió para preparar la información extraída de la evidencia.

Una herramienta útil para evaluar la evidencia obtenida y formular conclusiones y recomendaciones es una hoja de hallazgos de auditoría. Esta herramienta permite a los auditores determinar si los hallazgos y recomendaciones se basan en evidencia suficiente e idónea, cuando ello corresponda.

3.2.6. Conclusiones de Auditoría

Las conclusiones de auditoría resumen el resultado del trabajo realizado y establecen si los objetivos de auditoría han sido alcanzados. Sin conclusiones apropiadas, el trabajo es incompleto. Todas las conclusiones de auditoría deben ser revisadas por un miembro experimentado del equipo, de mayor jerarquía que aquel que las preparó, pues tienen como propósito preparar el informe a base de la evaluación de:

- Las observaciones derivadas de los procedimientos de auditoría aplicados.
- Los hallazgos importantes de cada componente examinado.
- Los hallazgos de la auditoría obtenidos.

3.2.7. Papeles de Trabajo

Los resultados obtenidos en esta fase se documentarán en un expediente de papeles de trabajo, relacionados con la evidencia sustentatoria acumulada que respalde los hallazgos, conclusiones y recomendaciones.

La normativa técnica de auditoría está relacionada directamente con la documentación de la auditoría o la elaboración de papeles de trabajo, cuyo propósito es evidenciar o sustentar las conclusiones y opiniones contenidas en el informe de auditoría.

La auditoría es un proceso continuo de acumulación de información documental, testimonial, analítica y física relacionada con la verificación de las actividades desarrolladas por una entidad y el cumplimiento de las funciones y obligaciones de sus servidores y servidoras dirigidas a evaluar la eficiente utilización de los recursos, la efectividad en el logro de las metas y objetivos institucionales y el cumplimiento de las disposiciones legales, reglamentarias y normativas aplicables.

Los siguientes criterios se aplicarán para documentar una auditoría específica:

- Definir la estructura de los papeles de trabajo al iniciar la auditoría con base a los componentes definidos en el programa de trabajo.
- Estructurar el contenido de los papeles de trabajo por cada componente relevante que incluya varias actividades relacionadas.
- Utilizar de manera consistente los índices definidos en los componentes identificados.
- Desglosar en varios expedientes por componentes de acuerdo a la ejecución del trabajo para facilitar el manejo de la información y la documentación de la auditoría a nivel de los miembros del equipo.
- Mantener expedientes independientes de las fases hasta concluir la auditoría informática, acumulando la información al preparar el informe y presentar los resultados a la administración de la entidad.

- Agrupar los expedientes en legajos de información manejable para archivo y consulta posterior.
- Concluida la auditoría proceder a numerar y a referenciar todos los papeles de trabajo, partiendo del expediente de administración de la auditoría y los resultados obtenidos de la evaluación del control interno y en la ejecución del trabajo.
- Mantener en forma separada el expediente de papeles de trabajo de la supervisión técnica aplicada durante la auditoría informática y su archivo junto a la documentación de la auditoría.

3.3. COMUNICACIÓN DE RESULTADOS PROVISIONALES

Los hallazgos de auditoría informática se refieren a deficiencias o irregularidades identificadas, como consecuencia de la aplicación de los procedimientos de auditoría.

En el transcurso de una auditoría informática, los auditores mantendrán constante comunicación con los servidores, ex servidores y demás personas vinculadas con la acción de control, dándoles oportunidad de presentar pruebas documentadas, así como información escrita relacionada con la acción de control.

Los resultados provisionales de cada parte de la auditoría se darán a conocer tan pronto como se concreten, con la siguiente finalidad:

- Ofrecer la oportunidad para que se presenten justificativos debidamente fundamentados.

- Hacer posible que los auditores gubernamentales dispongan durante el desarrollo del trabajo de campo, de toda la documentación y evidencia relacionadas con la auditoría.

- Posibilitar que se presente información o evidencia adicional, en los términos y plazos establecidos en las disposiciones legales vigentes.
- Facilitar la implantación de las recomendaciones que, de conformidad con las disposiciones del organismo de control, deben ser aplicadas de manera inmediata y con carácter obligatorio por parte del titular y servidores responsables.

Los productos obtenidos en la fase de comunicación de resultados, serán sometidos a control de calidad, conforme a los procedimientos establecidos, a fin de garantizar que su contenido se ajuste a las políticas y normas de auditoría gubernamental emitidas por la Contraloría General del Estado. El control de calidad estará a cargo de profesionales que no intervinieron en la fase.

El equipo de auditoría comunicará los resultados provisionales en los términos y plazos establecidos en las disposiciones legales vigentes, a fin de que los servidores relacionados expongan sus puntos de vista y/o presenten documentación de descargo, en ejercicio de su derecho a la defensa, mismos que se considerarán en el Borrador del Informe, que será analizado en la conferencia final, por los auditores gubernamentales actuantes, los representantes de la entidad objeto de la auditoría y todas las personas vinculadas.

De ser el caso, a petición de la entidad se podrá efectuar una reunión de trabajo a fin de realizar aclaraciones sobre los hallazgos comunicados.

Asimismo, los auditores están obligados a preservar la confidencialidad de los procedimientos y resultados frente a terceros o a quienes no participen en la administración y ejecución de la acción de control, de conformidad con la normativa emitida para el efecto.

3.4. INFORME DE AUDITORÍA

El resultado de la auditoría informática implica la elaboración de un informe con los comentarios, conclusiones y recomendaciones pertinentes, en el que se

incluirán los puntos de vista y descargos entregados por los servidores, ex servidores y terceros.

El informe de auditoría es considerado de importancia ya que permite conocer si la entidad está logrando las metas y objetivos propuestos, si lo hace de manera eficiente, salvaguardando los recursos públicos y si está cumpliendo con las disposiciones legales vigentes.

El informe cumplirá con las características de utilidad y oportunidad, objetividad e imparcialidad, concisión, precisión, razonabilidad, sustento técnico-documental adecuado, tono constructivo, relevancia del contenido y claridad expositiva.

En el informe se considerará la priorización de los hallazgos de auditoría, que implica clasificarlos en rangos conforme a su importancia, con base en criterios objetivos y técnicos.

Para asignar la prioridad correspondiente, se tomará en cuenta los siguientes elementos:

- Importancia relativa del hallazgo: grado en que la deficiencia afecta el cumplimiento de los objetivos institucionales.

- Impacto real: magnitud de las consecuencias que generó la deficiencia.

- Propósito y alcance de la auditoría: nivel de alineación del hallazgo con los objetivos definidos en la etapa de planificación, así como su relevancia dentro del contexto de la auditoría realizada.

Las recomendaciones contenidas en el informe tienen como finalidad proporcionar asesoría a la máxima autoridad y a los funcionarios de la entidad examinada para el cumplimiento de sus funciones y responsabilidades. Estas recomendaciones buscan promover y controlar el uso eficiente y eficaz de los

recursos públicos, en concordancia con la misión de la CGE y uno de los principios de la INTOSAI, que establece la razón de ser de la fiscalización pública que es "crear valor para los ciudadanos".

En tal virtud, el informe debe ser elaborado con profesionalismo, cuidando tanto su presentación como su estructura y contenido, y deberá ajustarse a la normativa legal vigente aplicable al proceso de elaboración, trámite y aprobación de los informes de Auditoría Gubernamental.

SIGLAS Y ABREVIATUAS UTILIZADAS

BCP: Plan de Continuidad del Negocio

CGE: Contraloría General del Estado

CISO: Director de Seguridad de la Información

COBIT: Objetivos de Control para Tecnología de Información y Tecnologías Relacionadas

CPD: Centro de Procesamiento de Datos

DRP: Plan de Recuperación ante Desastres

EFS: Entidad Fiscalizadora Superior

EGSI: Esquema Gubernamental de Seguridad de la Información

INTOSAI: International Organization of Supreme Audit Institutions

ISACA: Asociación de Auditoría y Control de Sistemas de Información

ISO/IEC: International Organization for Standardization ó International Electrotechnical Commission, en inglés

ISSAI: Normas Internacionales para Entidades Fiscalizadoras Superiores

ITIL: Biblioteca de Infraestructura de Tecnologías de la Información o Information Technology Infrastructure Library, en inglés

LOPDP: Ley Orgánica de Protección de Datos Personales

LOSNCP: Ley Orgánica del Sistema Nacional de Contratación Pública

MINTEL: Ministerio de Telecomunicaciones y de la Sociedad de la Información

NIST: Instituto Nacional de Normas y Tecnología

OLA: Acuerdo de Nivel Operativo

RACI: Matriz de Asignación de Responsabilidades (Responsable, Aprobador, Consultado e Informado)

RPO: Punto Objetivo de Recuperación

RTO: Tiempo Objetivo de Recuperación

SERCOP: Servicio Nacional de Contratación Pública

SINARDAP: Sistema Nacional de Registro de Datos Públicos

SLA: Acuerdo de Nivel de Servicio

TAACS:	Técnicas de Auditoría Asistidas por Computador
TI:	Tecnología de la información
TIC:	Tecnología de la información y Comunicación
UC:	Contrato de Soporte
UPS:	Sistema de Alimentación Ininterrumpida

GLOSARIO DE TÉRMINOS

Aplicativo: Programa informático diseñado como herramienta para permitir a los usuarios realizar uno o diversos tipos de trabajo.

Base de datos: Programa capaz de almacenar gran cantidad de datos, relacionados y estructurados, que pueden ser consultados rápidamente de acuerdo con las características selectivas que se deseen.

CISO: Denominado también Director de Seguridad de la Información, quien es el encargado de la seguridad de la información de una entidad, para la protección de datos, activos y sistemas de amenazas internas y externas.

Dirección IP: Es una dirección única que identifica a un equipo dentro de una red o el Internet, está compuesta por 4 segmentos de números entre 0 y 255, separados por un punto.

IaaS: Infraestructura como Servicio, es un modelo de computación de servicios en la nube que ofrece recursos de infraestructura informática como servidores, almacenamiento y redes a través de internet, como un servicio bajo demanda.

Login: Proceso que controla el acceso individual a un sistema informático.

OLA: Acuerdo de Nivel Operacional (OLA, por sus siglas en inglés), es un contrato interno entre un proveedor de servicios de TI y otras partes de la misma organización que describe cómo se prestarán los servicios internos para apoyar los Acuerdos de Nivel de Servicio (SLA) acordados con los clientes externos.

PaaS: Plataforma como Servicio, en inglés (Platform as a Service), modelo de computación que ofrece una plataforma en la nube para desarrollar, implementar, ejecutar y gestionar aplicaciones.

RACI: Herramienta para la gestión de proyectos y procesos, que permite definir y comunicar los roles y responsabilidades de los diferentes miembros de un equipo en relación con las tareas y actividades de un proceso o proyecto.

Ransomware: Es un malware que impide al usuario acceder a la información, que a través de una extorsión los criminales piden fuertes cantidades de dinero para liberar las restricciones de acceso a la información.

SaaS: Software como Servicio, modelo de distribución de software en las que las aplicaciones son alojadas y gestionadas por un proveedor externo, y a las que los usuarios acceden a través de internet, en lugar de instalar y mantener el software en la infraestructura tecnológica de propiedad de la entidad.

SLA: Service Level Agreement o Acuerdo de Nivel de Servicio, constituye un contrato formal entre un proveedor de servicios y un cliente en el cual se define el nivel de servicio esperado y las responsabilidades de las partes.

Software: Es un conjunto de programas, instrucciones y reglas informáticas que permiten ejecutar distintas tareas.

Web: Vocablo en inglés que significa "red" o "malla". Este término forma parte de lo que se conoce como World Wide Web (www) que es la red informática que se emplea en todo el mundo.

REFERENCIAS BIBLIOGRÁFICAS

- Constitución de la República del Ecuador.
- Ley Orgánica de la Contraloría General del Estado y su Reglamento.
- Ley Orgánica de Protección de Datos Personales (LOPDP).
- Ley Orgánica del Sistema Nacional de Contratación Pública LOSNCP.
- Ley Orgánica para la Optimización y Eficiencia de Trámites Administrativos.
- Ley de Comercio Electrónico, Firmas y Mensajes de Datos y su Reglamento.
- Esquema Gubernamental de Seguridad de la Información (EGSI).
- Normas de Control Interno para las Entidades, Organismos del Sector Público y de las Personas Jurídicas de Derecho Privado que dispongan de recursos públicos.
- Norma Técnica de Interoperabilidad del Registro de Datos Públicos.
- Página web oficial de ISACA (Information Systems Audit and Control Association), https://www.isaca.org/, organismo internacional referente en el área de la auditoría informática que apoya el desarrollo de metodologías y certificaciones para la realización de actividades de auditoría y control en sistemas de información.
- ISO (2021). *ISO/CEI 27001 gestión de la seguridad de la información*. Recuperado de https://www.iso.org.
- COBIT 5 del año 2012 y COBIT 2019. *Objetivos de Control para las tecnologías de la información.* Recuperado de https://www.isaca.org/.
- EGSI, *ACUERDO MINTEL-MINTEL-2024-0003*, *Esquema Gubernamental de Seguridad de la Información – EGSI*.
- WGITA – MANUAL DE LA IDI SOBRE AUDITORÍA DE TI PARA ENTIDADES FISCALIZADORAS SUPERIORES, Revisión 2022. Elaborado por INTOSAI DEVELOPMENT INITIATIVE.
- Manual de Auditoría Gubernamental, Contraloría General del Estado.
- Reglamento para la elaboración, trámite y aprobación de informes de auditoría gubernamental, Contraloría General del Estado.

ANEXOS

ANEXO 1. MARCO LEGAL Y NORMATIVO

ANEXO 2. FUNCIONES Y RESPONSABILIDADES

ANEXO 3. CUESTIONARIO DE EVALUACIÓN DE CONTROL INTERNO AL COMPONENTE "DESARROLLO DE SISTEMAS"

ANEXO 4. MATRIZ DE EVALUACIÓN Y CALIFICACIÓN DEL RIESGO AL COMPONENTE "DESARROLLO DE SISTEMAS"

ANEXO 5. FORMATO DOCUMENTO DE PLANIFICACIÓN

ANEXO 6. PROGRAMA DE AUDITORÍA INFORMÁTICA

ANEXO 7. FORMATO PLAN DE PRUEBAS DE AUDITORÍA INFORMÁTICA

ANEXO 8. PRUEBAS PARA LA EJECUCIÓN DE LA AUDITORÍA INFORMÁTICA

ANEXO 9. HOJA DE HALLAZGO

MARCO LEGAL Y NORMATIVO

Las normas constituyen una fuente primaria de criterios de auditoría, traducidas en controles, indicadores y umbrales, siendo importante considerar las disposiciones sectoriales específicas que cada entidad auditada tiene de acuerdo a su misión, ya que estas rigen sus procesos, sistemas y servicios tecnológicos, y el desconocimiento de las mismas, comprometería la relevancia de los resultados obtenidos, de ahí la necesidad de que el equipo auditor identifique, analice y documente toda regulación aplicable al ente auditado.

Normativa nacional aplicable

En los artículos 211 y 212 de la Constitución de la República del Ecuador se establecen las competencias asignadas a la Contraloría General del Estado, respecto al control de la utilización de los recursos estatales y la consecución de los objetivos de las instituciones del Estado y de las personas jurídicas de derecho privado que dispongan de recursos públicos, y entre sus funciones se encuentra, dirigir el sistema de control administrativo que se compone de auditoría interna, auditoría externa y del control interno, así como expedir la normativa para el cumplimiento de sus funciones. Este accionar se sustenta en el artículo 226 de la Constitución, que dispone que las instituciones del Estado deben actuar dentro del ámbito de sus competencias, coordinar acciones para el cumplimiento de sus fines y garantizar el goce y ejercicio de los derechos reconocidos constitucionalmente.

Adicionalmente, es necesario observar los artículos 76 numerales 3 y 4, 83 numeral 8, 100 numeral 4 y 233 de la Constitución de la República del Ecuador, que establecen derechos, garantías y responsabilidades referentes al patrimonio del Estado, la transparencia y el buen uso de los recursos públicos.

Las instituciones del Estado, sus dignatarios, autoridades, funcionarios y demás servidores, actuarán dentro del Sistema de Control, Fiscalización y Auditoría del Estado, cuya aplicación propenderá a que, sin excepción, se responsabilicen y

rindan cuentas públicas sobre el ejercicio de sus atribuciones, la utilización de los recursos públicos puestos a su disposición, así como, de los resultados obtenidos de su empleo.

La Ley Orgánica de la Contraloría General del Estado, faculta la ejecución de auditorías informáticas en los siguientes términos:

> ***"Auditoría informática**: Se enfoca en el control de los recursos informáticos de las entidades, organismos del sector público y de las personas jurídicas de derecho privado que dispongan de recursos públicos para evaluar su eficiencia y efectividad. Esta modalidad de control examinará y verificará los sistemas, las aplicaciones, infraestructura y procesos de tecnología de la información para identificar y corregir vulnerabilidades, incumplimientos y riesgos que puedan afectar a la integridad, la confidencialidad, la disponibilidad de la información y los recursos informáticos, a fin de evitar fuga de información que pueda afectar a la integridad de los recursos públicos. Esta modalidad de auditoría concluirá con el informe correspondiente que contendrá los comentarios, conclusiones y recomendaciones pertinentes.*"

El Ministerio de Telecomunicaciones y de la Sociedad de la Información (MINTEL) creado con el objetivo de impulsar el desarrollo de las telecomunicaciones y la sociedad de la información en el país, ha emitido normativa encaminada a modernizar y controlar la infraestructura tecnológica, y promover la transformación digital, mediante la emisión de los siguientes instrumentos:

- Esquema Gubernamental de Seguridad de la Información (EGSI), que constituye un marco normativo obligatorio para la gestión de la seguridad de la información en instituciones públicas, basado en la identificación y tratamiento de riesgos, con controles alineados a estándares internacionales como son la ISO/IEC 27001 y ISO/IEC 27002.

- Política Nacional de Ciberseguridad, define la estrategia nacional de ciberseguridad, incluyendo la protección de infraestructuras críticas y la coordinación con el Centro de Respuestas a Incidentes Informáticos EcuCERT de la Agencia de Regulación y Control de las Telecomunicaciones (ARCOTEL), siendo su función principal proteger la seguridad cibernética de las redes de telecomunicaciones del país, mediante la detección, análisis y respuesta a incidentes de ciberseguridad.

- Política para el uso de Servicios en la Nube en el Sector Público, regula el uso de servicios en la nube para este sector en referencia, con el fin de promover la adopción segura y eficiente de esta tecnología, maximizando los beneficios y minimizando los riesgos asociados a su uso, considerando la protección de datos, la privacidad y la seguridad de la información.

- Norma Técnica para la Aprobación de Viabilidad Técnica de Proyectos de Gobierno Electrónico, con los procedimientos y requisitos que deben cumplir las entidades del sector público para la aprobación de viabilidad técnica de proyectos de gobierno electrónico, y para la autorización de criticidad de software y servicios relacionados.

- Reglamento para la Adquisición de Software por las Entidades Contratantes del Sector Público, establece las clases de prelación en la adquisición de software por parte de las entidades que pertenecen a este sector, priorizando el uso de software de código abierto con componente mayoritario de valor agregado ecuatoriano.

La Ley Orgánica de Protección de Datos Personales (LOPDP), establece principios y obligaciones para el tratamiento lícito y protección de datos personales, con este propósito, regula, prevé y desarrolla principios, derechos, obligaciones y mecanismos que permitan verificar la confidencialidad y consentimiento de uso de la información personal contenidos en cualquier tipo de soporte.

La Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos (LCEFEYMD) y su Reglamento general (RLCE), regulan los mensajes de datos, la firma electrónica, los servicios de certificación, la contratación electrónica y telemática, la prestación de servicios electrónicos, a través de redes de información, incluido el comercio electrónico y la protección a los usuarios de los sistemas empleados para estos servicios.

La Ley Orgánica del Sistema Nacional de Contratación Pública (LOSNCP), su Reglamento General y las Resoluciones emitidas por el SERCOP, establecen la conformación y funcionamiento del Sistema Nacional de Contratación Pública, determinan las normas para regular los procedimientos de contratación para la

adquisición o arrendamiento de bienes, ejecución de obras y prestación de servicios, incluidos los de consultoría; y, los principios de legalidad, trato justo, igualdad, calidad, vigencia tecnológica, oportunidad, concurrencia, transparencia, publicidad; y, participación nacional.

La Norma Técnica de Interoperabilidad del Registro de Datos Públicos**,** emitida por la Dirección Nacional de Registros Públicos (DINARP), que regula el intercambio electrónico de información entre instituciones públicas mediante la plataforma de interoperabilidad SINARDAP.

La Ley Orgánica para la Optimización y Eficiencia de Trámites Administrativos, que dispone la optimización de trámites administrativos, regula su simplificación y reduce sus costos de gestión, con el fin de facilitar la interacción entre las y los administrados y la Administración Pública y entre las entidades que la componen; así como, garantizar el derecho de las personas a contar con una Administración Pública eficiente, eficaz, transparente y de calidad.

Las Normas de Control Interno para las Entidades, Organismos del Sector Público y de las Personas Jurídicas de Derecho Privado que dispongan de recursos públicos (NCI-CGE), secciones 100, 200, 300 y 410 "Tecnologías de la Información", propician con su aplicación, el mejoramiento de los sistemas de control interno y la gestión pública, respecto a la utilización de los recursos públicos y la consecución de los objetivos institucionales**.**

Además, la normativa general y específica emitida por los organismos competentes que fuere aplicable.

Normativa y marco internacional aplicable

En el Manual de Auditoría Informática, se acogen estándares internacionales, marcos de referencia y buenas prácticas reconocidos mundialmente, siempre que no contravengan disposiciones legales nacionales, los cuales complementan la normativa nacional y ofrecen criterios objetivos para evaluar la gobernanza, la gestión y la seguridad de los sistemas de información y comunicaciones, los que permiten al auditor informático contar con criterios de madurez global que tienen las entidades que se encuentran bajo su control en

este ámbito, y adoptar técnicas de prueba validadas en otras Entidades Fiscalizadoras Superiores (EFS), que servirán para generar recomendaciones para la mejora de los procesos de las entidades gubernamentales.

- Las Normas Internacionales de las Entidades Fiscalizadoras Superiores ISSAI 100 y 5300 emitidas por la Organización Internacional de Entidades Fiscalizadoras Superiores (INTOSAI), constituyen principios fundamentales para la realización de auditorías de desempeño y directrices especializadas en TI.

- Las normas internacionales ISO/IEC 27001:2022 que definen los requisitos para establecer, implementar, mantener y mejorar de manera continua el Sistema de Gestión de Seguridad de la Información (SGSI), e ISO/IEC 27002:2022, constituye la guía de implementación de los controles de seguridad de la información, las dos tienen como finalidad minimizar riesgos, accesos no autorizados, posibles daños financieros y de reputación; estas dos normas son la base del EGSI y Normas de Control Interno de la CGE, por lo tanto, fuente de criterios de evaluación para las auditorías informáticas.

- La ISO 27032 que se enfoca en la ciberseguridad, proporcionando directrices y mejores prácticas para garantizar la seguridad de la información en las conexiones de redes y transferencia de información; la norma se aplica a diversas áreas de la ciberseguridad, incluida la seguridad en la nube.

- La ISO/IEC 22301 para la gestión de la continuidad y resiliencia organizacional; entrega los requisitos para implementar, mantener y mejorar un sistema de gestión para protegerse contra, reducir la probabilidad de ocurrencia de, prepararse para responder a, y recuperarse de disrupciones que puedan surgir; siendo genérica se espera al auditar que las entidades hayan adoptado un marco de continuidad operacional; como lo señala el EGSI v3.0 en (1.30) acerca de la preparación de las TIC para la continuidad, lo enumerado en ese apartado es sólo una parte clave de los requisitos de la continuidad de la organización.

- ITIL v4, marco de referencia para la gestión de servicios de TI, que presenta un modelo de cuatro dimensiones: organizaciones y personas, información y tecnología, socios y proveedores, y flujos de valor y procesos.

- WGTIA, el manual propuesto por el Grupo de Trabajo sobre Auditoría de TI de la INTOSAI para la aplicación por parte de las EFS.

- GTAG (IIA) – Guías de Auditoría de TI, constituyen orientaciones prácticas para auditorías específicas (ciberseguridad, cambio de aplicaciones, CAATs, etc.).

- COBIT, marco de referencia desarrollado por ISACA (Information Systems Audit and Control Association), reconocido y aplicado internacionalmente, comprende cinco componentes principales: un sistema de objetivos, componentes de gobierno y gestión, un modelo de evaluación de desempeño, una guía de diseño de sistema de gobierno y descripciones de roles, actividades y relaciones de gobierno, a través de los cuales se gestionan los riesgos y mejoras de los controles de TI.

- NIST SP 800-53 Rev. 5, marco de referencia de ciberseguridad desarrollado por el Instituto Nacional de Estándares y Tecnología (NIST) de EE.UU., proporciona un catálogo de controles de seguridad y privacidad para los sistemas de información, de importancia para la seguridad de infraestructuras críticas o convenios internacionales.

Jerarquía normativa

De conformidad con lo dispuesto en el artículo 425 de la Constitución de la República del Ecuador, el orden jerárquico de aplicación de las normas será la siguiente manera: la Constitución; los tratados y convenios internacionales; las leyes orgánicas; las leyes ordinarias; las normas regionales y las ordenanzas distritales; los decretos y reglamentos; las ordenanzas; los acuerdos y las resoluciones; y, los demás actos y decisiones de los poderes públicos. En caso de conflicto entre normas de distinta jerarquía, la Corte Constitucional, las juezas y jueces, autoridades administrativas y servidoras y servidores públicos, lo resolverán mediante la aplicación de la norma jerárquica superior.

La jerarquía normativa considerará, en lo que corresponda, el principio de competencia, en especial la titularidad de las competencias exclusivas de los gobiernos autónomos descentralizados.

En ese sentido, durante el desarrollo de la acción de control el equipo auditor, de ser el caso, observará la jerarquía normativa dispuesta en la Constitución.

FUNCIONES Y RESPONSABILIDADES

Realizar una adecuada definición de funciones y responsabilidades de los integrantes del equipo auditor, permite una ejecución ordenada, objetiva y eficiente del proceso, asegurando el cumplimiento de los objetivos establecidos, el respeto a los principios de auditoría y el uso responsable de los recursos asignados.

Dada la naturaleza técnica y especializada de la auditoría informática, el equipo puede estar conformado por profesionales de distintas disciplinas, tales como ingeniería en sistemas, auditoría, derecho, administración, seguridad de la información, medicina, entre otros. Cada perfil aporta una perspectiva complementaria, lo que permite un análisis integral y contextualizado.

A continuación, se detallan las funciones generales y responsabilidades específicas de los integrantes del equipo de auditoría informática, en concordancia con los principios de independencia, objetividad, competencia profesional y confidencialidad:

a) Director/a
b) Apoyo especializado (Financiero, legal, mecánico, eléctrico, TTHH, entre otros)
c) Apoyo Informático
d) Auditor Operativo
e) Jefe de Equipo
f) Supervisor
g) Supervisor General de Calidad

a) Director/a: Responsable de la unidad de control, que cumplirá las siguientes responsabilidades:

- Elaborar la planificación anual de la auditoría de acuerdo con el ámbito asignado, en coordinación con las unidades administrativas correspondientes.

- Organizar equipos de auditoría para realizar los exámenes programados, tomando en cuenta para su integración, entre otros aspectos, las condiciones técnicas, conocimiento, experiencia, habilidades y relaciones
  interpersonales.
- Programar las auditorías a base de los criterios y estándares mínimos, tales como el objetivo general, el alcance, el tiempo para su ejecución, número de auditores por equipo y las instrucciones específicas, entre otros.
- Apoyar e incentivar la participación activa de los auditores, con el propósito de lograr el objetivo general propuesto para la auditoría específica.
- Prestar a los supervisores y auditores asignados para la ejecución del trabajo, la asistencia técnica necesaria para que éstos cumplan eficientemente con sus obligaciones.
- Conocer y aprobar el informe sobre la planificación preliminar y la planificación específica previa a la ejecución del trabajo y examen de áreas críticas.
- Exigir la aplicación sistemática del proceso de la auditoría a base de la metodología definida para el efecto, en todos aquellos trabajos cuya naturaleza, objetivo y alcance lo ameriten.
- Fomentar la aplicación de las políticas y normas de auditoría emitidas por la Contraloría General, como garantía de la calidad del trabajo.
- Suscribir, cuando corresponda, los informes de auditoría o de examen especial, que serán remitidos a la administración de las entidades examinadas.
- Preparar un informe final con los resultados obtenidos en la ejecución del plan anual de trabajo.
- Supervisar selectivamente el funcionamiento técnico y administrativo de los equipos de trabajo ubicados en las entidades auditadas, como un criterio para fomentar el control de calidad interno.
- Cumplir y hacer cumplir las disposiciones legales reglamentarias y la normatividad relacionada con el control de los recursos públicos emitida por la Contraloría General del Estado.

b) Apoyo especializado: Profesional no informático que brinda apoyo en áreas que requieren conocimientos específicos para el análisis de los procesos automatizados a través de los sistemas y aplicaciones informáticas. Las responsabilidades que tendrá conforme el programa de auditoría asignado serán las siguiente:

- Aplicar el programa de auditoría preparado por el Jefe de Equipo y supervisor.
- Documentar la aplicación de los procedimientos de auditoría utilizando la estructura y orden definido para la elaboración de los papeles de trabajo.
- Elaborar y entregar los informes técnicos de manera formal con los resultados y conclusiones del análisis efectuado y documentación de sustento.
- Cumplir con los criterios de ejecución establecidos para su trabajo, así como, los estándares profesionales (normas de auditoría) y de encontrar dificultades, comunicarlas de inmediato al auditor jefe de equipo de la auditoría.
- Mantener ordenados y completos los papeles de trabajo.
- Sugerir procedimientos alternativos o adicionales para promover la eficiencia en las actividades de auditoría realizadas.
- Colaborar continuamente para fomentar el logro de los objetivos incluidos en la planificación específica y contribuir para proyectar una imagen positiva de la auditoría y de la Contraloría.
- Cumplir con las disposiciones legales, normatividad e instrucciones relacionadas con el ejercicio de la auditoría, así como observar el Código de Ética Profesional y mantener la confidencialidad de la información de la entidad y la generada por el equipo de auditoría.

c) Apoyo Informático: Profesional con conocimientos en tecnologías de la información y comunicaciones, que interviene de forma temporal y específica para el análisis de aspectos informáticos, orientado a asistir al equipo de auditoría de otras unidades de control que efectúan un examen diferente al de auditoría informática.

Las responsabilidades que tendrá conforme el programa de auditoría asignado serán las siguiente:

- Aplicar el programa de auditoría preparado por el Jefe de Equipo y supervisor.
- Documentar la aplicación de los procedimientos de auditoría utilizando la estructura y orden definido para la elaboración de los papeles de trabajo.
- Elaborar y entregar los informes técnicos de manera formal con los resultados y conclusiones del análisis efectuado y documentación de sustento.
- Cumplir con los criterios de ejecución establecidos para su trabajo, así como, los estándares profesionales (normas de auditoría) y de encontrar dificultades, comunicarlas de inmediato al auditor jefe de equipo de la auditoría.
- Mantener ordenados y completos los papeles de trabajo.
- Sugerir procedimientos alternativos o adicionales para promover la eficiencia en las actividades de auditoría realizadas.
- Colaborar continuamente para fomentar el logro de los objetivos incluidos en la planificación específica y contribuir para proyectar una imagen positiva de la auditoría y de la Contraloría.
- Cumplir con las disposiciones legales, normatividad e instrucciones relacionadas con el ejercicio de la auditoría, así como observar el Código de Ética Profesional y mantener la confidencialidad de la información de la entidad y la generada por el equipo de auditoría.

d) Auditor Operativo: Las responsabilidades serán entre otras, las siguiente:

- Aplicar los programas de auditoría preparados para el desarrollo del trabajo, conforme a las instrucciones del jefe de equipo.
- Documentar la aplicación de los procedimientos de auditoría utilizando la estructura y orden definido para los papeles de trabajo.
- Cumplir con los criterios de ejecución establecidos para su trabajo, así como, los estándares profesionales (normas de auditoría) y de encontrar dificultades, comunicarlas de inmediato al auditor jefe de equipo de la auditoría.
- Mantener ordenados y completos los papeles de trabajo.
- Sugerir procedimientos alternativos o adicionales para promover la eficiencia en las actividades de auditoría realizadas.

- Colaborar continuamente para fomentar el logro de los objetivos incluidos en la planificación general y contribuir para proyectar una imagen positiva de la auditoría y de la Contraloría General del Estado.
- Obtener la evidencia suficiente, competente y pertinente de los hallazgos de auditoría, desarrollando los comentarios con todos los atributos y analizarlos con el Jefe de equipo de la auditoría.
- Elaborar las hojas de hallazgo con su documentación de soporte, misma que incluirá la condición, criterio, causa y efecto, e identificación de las personas relacionados con el hallazgo.
- Estructurar el expediente de papeles de trabajo y entregarlo al jefe de equipo para su inclusión en el expediente de la auditoría.
- Mantener actualizada la información de las actividades de ejecución de la auditoría en los aplicativos institucionales.

  Cumplir con las disposiciones legales, normatividad e instrucciones relacionadas con el ejercicio de la auditoría, así como observar el Código de Ética Profesional y mantener la confidencialidad de la información de la entidad y la generada por el equipo de auditoría.

e) Jefe de equipo: Las responsabilidades serán entre otras, las siguiente:

- Ejecutar de manera conjunta con el supervisor las funciones de responsabilidad compartida.
- Elaborar conjuntamente con el supervisor la planificación general.
- Administrar la acción de control sobre la base de la orden de trabajo emitida.
- Ejecutar y controlar las actividades inherentes a la planificación, ejecución y comunicación de resultados de las acciones de control.
- Establecer lineamientos para la ejecución de la acción de control al equipo a su cargo, controla y evalúa su aplicación.
- Incentivar la participación activa de los miembros del equipo para el cumplimiento de los objetivos de la auditoría.
- Revisar y elaborar las notificaciones y comunicaciones a los servidores y ex servidores relacionados en la acción de control.
- Elaborar el informe de evaluación del sistema de control interno de la entidad u organismo auditado.
- Participar en reuniones de trabajo inherentes a la acción de control en ejecución.

- Registrar y documentar la información de la acción de control en los sistemas informáticos.
- Ejecuta y elaborar el informe de verificación preliminar.

f) Supervisor: Las responsabilidades serán entre otras, las siguiente:

- Preparar y aplicar los programas de supervisión, en las principales etapas del proceso de la auditoría.
- Desarrollar conjuntamente con el Jefe de equipo de auditoría, las funciones
  de responsabilidad compartida, especialmente las relacionadas con la planificación general.
- Supervisar la elaboración del informe sobre requerimientos de ampliaciones de plazo, inclusión y exclusión del personal de los equipos de auditoría; y, sobre requerimientos para modificaciones a los alcances de las acciones de control en ejecución; y, para suspensiones temporales y cancelaciones de acciones de control.
- Supervisar y ejecutar las actividades de las distintas fases de la auditoría, de conformidad con la orden de trabajo asignada.
- Establecer lineamientos para el equipo de auditoría para la ejecución de la acción de control.
- Supervisar periódicamente las actividades del equipo de auditoría, de acuerdo con la fase del proceso de la auditoría que se esté realizando, para orientar los procedimientos, evaluar el avance del trabajo, resolver las consultas realizadas, revisar los productos intermedios y finales del trabajo, informar a la jefatura sobre los asuntos importantes de la auditoría informática, así como los de carácter administrativo, y elabora hojas de supervisión de la acción de control.
- Supervisar el reporte de labores y avance de trabajo de los integrantes de los equipos de trabajo asignados.
- Supervisar la elaboración y ejecución de programas de trabajo, matrices de riesgos y evaluación del sistema de control interno.
- Supervisar la elaboración de las convocatorias para lectura del borrador de informe, acta de comunicación de resultados del informe de la acción de control.
- Participar en las reuniones programadas de lectura del borrador de informe.

- Supervisar los documentos de planificación, comunicación de resultados provisionales, borrador de informe, informe para aprobación y todo el archivo de sustento para su aprobación conforme la normativa legal vigente.

g) **Supervisor General de Calidad:** Las responsabilidades serán entre otras, las siguiente:
   - Propone la conformación de los equipos que efectuarán las acciones de control.
   - Analiza e informa al Director/a Nacional de Auditoría sobre requerimientos de ampliaciones de plazo, inclusión y exclusión del personal de los equipos de auditoría; y, sobre requerimientos para modificaciones a los alcances de las acciones de control en ejecución.
   - Supervisa y controla la aplicación de metodologías para la planificación, ejecución, supervisión, evaluación y elaboración de informes de las acciones de control.
   - Supervisa la calidad de la planificación de la acción de control.
   - Supervisa la calidad del borrador de informe de la acción de control, previo a la lectura del mismo.
   - Supervisa la calidad del informe de la acción de control y toda la documentación de sustento para su aprobación conforme la normativa legal vigente.
   - Realiza el control de calidad de los informes de verificación preliminar.

ANEXO 3. CUESTIONARIO DE EVALUACIÓN DE CONTROL INTERNO AL COMPONENTE "DESARROLLO DE SISTEMAS"

Anexo X - Evaluación de Control Interno de Auditoría Informática .....

CONTRALORÍA GENERAL DEL ESTADO

DIRECCIÓN NACIONAL DE AUDITORÍA xxx

COMPONENTE: Desarrollo del sistema XXX

N°	Cuestionario	PT	SI/NO	CT	Medio de Verificación	Observaciones
1. Estudio de factibilidad **Objetivo:** Verificar La viabilidad técnica, económica, legal, operativa del sistema a ser desarrollado o adquirido.		**4**		**2**		
1	¿Para el desarrollo del sistema XXX, existió el estudio de viabilidad técnica, legal, operativa y de tiempo?	1	SI	1	Documento de estudio de factibilidad técnica, legal y operativa para el desarrollo del sistema XXX	
2	Para el sistema XXX, se realizó un informe de análisis de mercado conforme a la solución tecnológica requerida, que permita determinar si desarrollar el mismo internamente o contratarlo?	1	NO	0	Informe aprobado del análisis de mercado correspondiente a la solución tecnológica	
3	¿Producto del estudio de factibilidad se elaboró un informe con las alternativas y soluciones propuestas incluido las recomendaciones para la toma de decisiones?	1	SI	1	Informe del estudio de factibilidad con las recomendaciones para la toma de decisiones por parte de las autoridades	
4	¿El estudio de factibilidad, consideró un plan de riesgos para el requerimiento de la solución tecnológica?	1	NO	0	Entrevistar a responsables de TI y cumplimiento para validar la aplicación práctica de la política.	

NC	RI
50%	50%
BAJO	ALTO

N°	Cuestionario	PT	SI/NO	CT	Medio de Verificación	Observaciones
2. Desarrollo y gestión de requisitos **Objetivo:** Verificar el establecimiento de la necesidad de la solución tecnológica, por parte del área interesada.		**3**		**1**		
1	¿Previo al desarrollo del sistema XXX, las partes interesadas elaboraron y formalizaron la documentación en la que constó la justificación de la necesidad para disponer del mencionado sistema?	1	SI	1	Documentó aprobado con la justificación de la necesidad para desarrollar el sistema.	
2	¿Existe como respaldo del desarrollo del sistema XXX, la documentación correspondiente al levantamiento de los requerimientos funcionales y técnicos, considerando la clasificación y priorización de los requisitos del mismo?	1	NO	0	Documentación del levantamiento de los requerimientos funcionales y técnicos para el desarrollo del sistema XXX Documento con clasificación y priorización de los requisitos establecidos	
3	¿Se elaboró y aprobó un informe de la evaluación de impacto de los requerimientos sobre la arquitectura, procesos y normativa de la entidad?	1	NO	0	Evaluación de selección y monitoreo	

NC	RI
33%	67%
BAJO	ALTO

N°	Cuestionario	PT	SI/NO	CT	Medio de Verificación	Observaciones
3. Diseño/Desarrollo **Objetivo:** Comprobar el establecimiento de las especificaciones de software, hardware y medios de conectividad, necesarios para el funcionamiento integral y despliegue de la solución tecnológica para su utilización		**4**		**0**		
1	¿Se elaboró y aprobó una arquitectura que soporte el desarrollo y operatividad del sistema XXX?	1	NO	0	Documento aprobado con la arquitectura para la implementación del sistema XXX	
2	¿Cómo parte del diseño del sistema XXX, se realizó un análisis de la definición de los componentes de software y hardware requeridos para la solución tecnológica propuesta?	1	NO	0	Documento con la definición de los componentes requerido de software y hardware requeridos para la solución tecnológica	
3	¿Para el desarrollo del sistema XXX, se establecieron los requisitos técnicos que incluyeron los procedimientos y estándares definidos por la entidad para el desarrollo de la solución a nivel de codificación o programación y diseño de base de datos?	1	NO	0	Documento aprobado de los estándar de desarrollo de sistemas tecnológicos.	
4	¿En el desarrollo del sistema XXX, se definieron e incluyeron pistas de auditoría para registrar las acciones de los usuarios de manera transparente en apego de la normativa legal vigente, garantizando la integridad y confiabilidad de los datos?	1	NO	0	Implementación de pistas de auditoría de la solución tecnológica.	

NC	RI
0%	100%
BAJO	ALTO

CT	3		NC/RI	**ENFOQUE**
PT	11		Preguntas evaluadas	
NC	27%		BAJO	**SUSTANTIVO**
RI	73%		ALTO	

Criterio de Evaluación	Riesgo		Nivel de confianza	
1. Estudio de factibilidad Objetivo: Verificar La viabilidad técnica, económica, legal, operativa del sistema a ser desarrollado o adquirido.	50%	ALTO	50%	BAJO
2. Desarrollo y gestión de requisitos Objetivo: Verificar el establecimiento de la necesidad de la solución tecnológica, por parte del área interesada.	100%	ALTO	33%	BAJO
3. Diseño/Desarrollo Objetivo: Comprobar el establecimiento de las especificaciones de software, hardware y medios de conectividad, necesarios para el funcionamiento integral y despliegue de la solución tecnológica para su utilización	0%	0	0%	BAJO
TOTAL	**73%**	**ALTO**	**27%**	BAJO

No	Hechos Reportables:	Posibles Responsables
1		
2		
3		
4		
5		

ANEXO 4. MATRIZ DE EVALUACIÓN Y CALIFICACIÓN DEL RIESGO AL COMPONENTE "DESARROLLO DE SISTEMAS"

CONTRALORÍA GENERAL DEL ESTADO

Componente: Desarrollo del sistema XXX

ELEMENTOS CLAVE	RIESGOS		FUNDAMENTO	CONTROLES CLAVES	ENFOQUE DE AUDITORÍA	
	INHERENTE	CONTROL			PRUEBAS DE CUMPLIMIENTO	PRUEBAS SUSTANTIVAS
1. Estudio de factibilidad	Alto	Alto	Riesgo Inherente: Personal técnico sin capacitación del uso de herramientas tecnológicas actualizadas para el desarrollo de soluciones informáticas. Alta rotación del personal del personal de tecnología de la información. Riesgos de Control: - Falta de un de análisis de mercado para determinar la factibilidad de desarrollar el sistema XXX a la medida o realizar una adquisición de la solución requerida. - Inexistencia de un plan de riesgos para determinar la factibilidad del desarrollo e implantación del sistema XXX, en función de los requerimientos solicitados.	- Realización obligatoria de un estudio de mercado. - Participación de un comité multidisciplinario en la toma de decisión. - Identificación temprana de riesgos desde la fase de análisis de requerimientos. - Matriz de riesgos del sistema con valoración de impacto y probabilidad. - Asignación de responsables y planes de contingencia/mitigación por cada riesgo identificado.	- Solicitar si en el análisis efectuad, todas las justificaciones de costos/beneficios son verificables	- Verificar la factibilidad legal, mediante la validación de cumplimiento de normativa aplicable a la solución tecnológica. - Verificar si se efectuó la evaluación de procesos actuales respecto a las nuevas soluciones tecnológicas o cambios propuestos, y su impacto en los procesos actuales. - Verificar si se contó con el análisis de costo beneficio mediante la comparación con otras soluciones de iguales características. - Verificar si se elaboró la matriz de riesgos, completo y su plan de acción.
2. Desarrollo y gestión de requisitos	Alto	Alto	Riesgo Inherente: - Falta de involucramiento de todas las partes interesadas, para el establecimiento de los requerimientos del sistema XXX. - Riesgos de seguridad no considerados desde la etapa de requisitos. Riesgos de Control: - Inexistencia de la documentación correspondiente al levantamiento de los requerimientos funcionales y técnicos. - Falta de un informe de la evaluación de impacto de los requerimientos sobre la arquitectura, procesos y normativa de la entidad.	- Uso obligatorio de formatos institucionales para levantamiento de requerimientos. - Aprobación formal de los requerimientos por parte de usuarios clave y áreas técnicas. - Inclusión del levantamiento de requerimientos como hito obligatorio en el cronograma del proyecto que comprende el desarrollo del sistema XXX. - Establecer la obligatoriedad de un informe formal de evaluación de impacto. - Incluir a áreas responsables de arquitectura empresarial, procesos y cumplimiento normativo.	- Solicitar la documentación de recolección de las necesidades, que incluya las expectativas, restricciones, interfases y todos los requisitos funcionales, no funcionales y normativos, para la implementación de los sistemas o aplicativos informáticos.	- Verificar la existencia de documentación del levantamiento de los requerimientos, como: la aplicación de listas de requerimientos, historias de usuario, casos de uso, diagramas de flujo, etc., definiciones formalizadas por las partes interesadas correspondientes; y, con documentación que evidencie los controles de cambio efectuados. - Evaluar si el sistema XXX cumplió con los requerimientos funcionales, y normativa que regula el proceso automatizado. - Revisar si se cuenta con documentación formalizada que evidencie la participación de todas las partes interesadas en las pruebas de aceptación, recepción y paso a producción de los sistemas o aplicaciones. - Verificar si se implementó los criterios y condiciones de interoperabilidad con otros sistemas internos y externos.
3. Diseño/Desarrollo	Alto	Alto	Riesgo Inherente: - Bajo conocimiento técnico y alta rotación del equipo informático designado para el diseño y desarrollo de la solución informática. - Infraestructura tecnológica desactualizada. - Personal técnico sin conocimientos actualizados en el uso de nuevas tecnologías de la información. Riesgos de Control: - Ausencia de una arquitectura tecnológica formalmente definida, documentada y aprobada para el sistema XXX. - Falta de análisis en la definición de los componentes de software y hardware requeridos para una solución tecnológica requerida. - Falta de procedimientos y estándares definidos por la entidad para el desarrollo de la solución a nivel de codificación o programación y diseño de base de datos, inexistente. - No se definieron e incluyeron pistas de auditoría para registrar las acciones de los usuarios de manera transparente en apego de la normativa legal vigente, garantizando la integridad y confiabilidad de los datos	- Definición formal y documentada de la arquitectura tecnológica del sistema XXX. - Aprobación oficial de la arquitectura por parte del área de arquitectura TI y gobernanza tecnológica. - Realización de un estudio técnico detallado para identificar componentes de software y hardware necesarios. - Elaboración de especificaciones técnicas documentadas y aprobadas del sistema - Definición y documentación formal de estándares de codificación y diseño de bases de datos. - Aprobación y difusión institucional de los procedimientos y estándares definidos y aprobados. - Establecimiento de políticas y procedimientos para la implementación de pistas de auditoría. - Definición clara de eventos críticos a auditar (acceso, modificaciones, eliminación, autorizaciones, etc.). - Implementación técnica de logs de auditoría en sistemas y bases de datos con formato estructurado y seguro.		- Verificar que se efectuó la definición de la arquitectura de datos y componentes de acuerdo con la normativa y definición de requerimientos funcionales. - Verificar si la definición de la arquitectura, incluyó el desglose de los componentes que involucran a más del sistema o aplicativo, software base, bases de datos, lenguajes de programación, infraestructura tecnológica con la capacidad de recursos requeridos. - Verificar si la arquitectura, incluyó la definición de las especificaciones técnicas de los equipos, aplicativos de seguridad y servicios de conectividad, entre otros componentes de TI requeridos para el funcionamiento, despliegue y operación de la solución. - Verificar si la codificación y desarrollo de programas y documentos se realizó utilizando las metodologías, estándares, procedimientos aprobados, validaciones generales y específicas de aplicación. - Verificar, si en el sistema XXX, se implementaron las pistas de auditoría pertinentes.

ANEXO 5. FORMATO DOCUMENTO DE PLANIFICACIÓN

CONTRALORÍA GENERAL DEL ESTADO

[NOMBRE DE LA UNIDAD DE CONTROL]

[NOMBRE DE LA ENTIDAD AUDITADA]

PLANIFICACIÓN GENERAL

AUDITORÍA INFORMÁTICA A [TIPOS DE AUDITORÍA INFORMÁTICA DEFINIDOS EN EL MANUAL …], EN [NOMBRE DE LA ENTIDAD AUDITADA], UBICADO/A EN LA [CIUDAD DE […], CANTÓN […], PROVINCIA DE […]], POR EL PERÍODO COMPRENDIDO ENTRE EL [DÍA, MES Y AÑO] Y EL [DÍA, MES Y AÑO].

PLANIFICACIÓN GENERAL

1. Identificación de la Entidad

ENTIDAD:	[Nombre de la Entidad Auditada]
CIUDAD:	[Ciudad donde se realiza la acción de control]
DIRECCIÓN:	[Dirección de ubicación de la Entidad Auditada]
TELÉFONO:	[Teléfono de la Entidad Auditada]
HORARIO DE TRABAJO:	[Horario de trabajo de la Entidad Auditada]
UBICACIÓN DEL EQUIPO DE AUDITORÍA:	[Ubicación de la oficina asignada al equipo para la ejecución de la auditoría en campo. Ejem.: Piso once del bloque azul del edificio matriz de la Plataforma Gubernamental de Gestión Financiera, ubicado en la Av. Amazonas entre Pereira y Unión Nacional de Periodistas, en la ciudad de Quito.]
SITIO WEB	[Sitio web del portal institucional de la Entidad auditada]

2. Motivo del examen

El examen especial en el [Nombre de la Entidad], se realiza en cumplimiento de la orden de trabajo [Nro. De Orden de Trabajo y fecha de emisión], con cargo al [Plan Anual de Control / Imprevistos] del año [año] de la [Nombre de la Unidad de Control].

3. Objetivos del examen

Los objetivos generales del examen especial son:

[Los constantes en la orden de trabajo]

4. Alcance de la auditoría

Comprende el análisis **[**describir los rubros y componentes tecnológicos, proceso de TI, período y aspectos relevantes que serán objeto de análisis en la auditoría**]**

5. Conocimiento de la Entidad y su base legal

5.1. Base Legal

[Descripción de la normativa con la cual se creó la Entidad auditada]

5.2. Principales disposiciones legales

[Detalle de la leyes y normativa relacionada con los componentes a analizar en la auditoría Ej.: Constitución de la República del Ecuador, Ley Orgánica del Sistema Nacional de Contratación Pública (LOSNCP) y su Reglamento General (RLOSNCP), de la normativa con la cual se creó la Entidad auditada]

5.3. Estructura Orgánica

[Descripción de Estatuto Orgánico aprobado de la entidad auditada y vigente durante el período de análisis del alcance de la auditoría; con la inclusión del cuadro con la descripción de los procesos en los diferentes niveles gobernantes y directivos, relacionados con los componentes a analizar de acuerdo al alcance de la auditoría. Ej.:]

Procesos	Numeral	Proceso / Unidad	Responsables
1.2 PROCESOS GOBERNANTES	**1.2.1.1.**	Direccionamiento Estratégico	Director/a General
1.3 PROCESOS SUSTANTIVOS	**1.3.1.1.**	Direccionamiento Técnico: Subdirección General	Subdirector/a General
	1.3.2.1.	Gestión Técnica de Catalogación	Coordinador/a Técnico/a de Catalogación
	1.3.2.1.1.	Gestión del Desarrollo de Catálogos	Director/a de Desarrollo de Catálogos
	1.3.2.1.2.	Gestión de Selección de Proveedores	Director/a de Selección de Proveedores
	1.3.2.1.3.	Gestión de Desarrollo de Compras Corporativas	Director/a de Desarrollo de Compras Corporativas

Procesos	Numeral	Proceso / Unidad	Responsables
	1.3.2.1.4.	Gestión de Administración de Catálogos y Gestión de Proveedores	Director/a de Administración de Catálogos y Gestión de Proveedores
	1.3.2.2.	Gestión Técnica de Control	Coordinador/a Técnico/a de Control

5.4. Organigrama

[Diagrama de la estructura orgánica definida en el estatuto vigente de la Entidad auditada]

5.5. Misión, Visión y Objetivos de la entidad

[Descripción de la misión, visión y objetivos de la entidad auditada]

5.6. Principales procesos relacionados con el alcance de la auditoría

[Descripción de los procesos de TI y de otras áreas de la Entidad con las cuales el equipo auditor mantendrá comunicación durante las actividades de control]

6. Seguimiento a recomendaciones

[Detallar y describir los informes de la Contraloría aprobados durante el período de análisis de auditoría con recomendaciones pendientes de cumplimiento realizadas a la entidad auditada relacionadas con los componentes de acuerdo al alcance de la orden de trabajo y que la CGE no haya efectuado su seguimiento en acciones de control anteriores.]

7. Monto de recursos examinados

[Determinar el monto de rubros que la auditoría efectuará su análisis, como aquellos constantes en los contratos de bienes y/o servicios de TI; o en caso de que los componentes no permitan determinar los montos, se sugiere el siguiente texto.

"… Del análisis realizado [componente de TI]; de acuerdo a su naturaleza, representan un monto indeterminado (…)"]

8. Servidores relacionados

[Cuadro o matriz con el detalle de los nombres y apellidos, cargos, período de actuación de los servidores identificado por el equipo de auditoría como

relacionados en los componentes y procesos de TI que serán objeto de análisis]

9. Evaluación del sistema de control interno y riesgos de auditoría

[Resultados obtenidas de la aplicación de la matriz de evaluación del control interno y análisis de riesgos]

10. Puntos de interés para la auditoría

[Descripción de los componentes y/o procesos sobre los cuales la auditoría en la fase de ejecución pondrá mayor interés en la aplicación de procedimientos por presentar mayor nivel de riesgos resultado de la evaluación de control interno.]

11. Condiciones reportables de la evaluación del sistema de control interno y riesgos de auditoría

[Descripción de las condiciones que podrían ser un potencial hallazgo de auditoría, resultado de la evaluación al control interno y análisis de riesgos, del cual se profundizará su análisis en la fase de ejecución.]

12. Plan de Muestreo

[De acuerdo a la naturaleza del componente y alcance del análisis se describirá el muestreo a efectuar en las pruebas sustantivas conforme la metodología propuesta en el manual de auditoría]

13. Programas de auditoría específicos a aplicarse en el examen

[Programas con los procedimientos a la medida por cada uno de los componentes a ser analizados de acuerdo al enfoque y alcance de la auditoría, que serán asignados a los auditores para su análisis]

14. Tiempo asignado y distribución del trabajo

[Detalle para cada integrante del equipo, las actividades y tiempos de cumplimiento en la auditoría, con las fechas tentativas de los hitos y productos, en cada fase de la auditoría]

15. Recursos a utilizarse

[Descripción de los integrantes del equipo de auditoría y personal del apoyo (técnico, legal) con la competencia técnica de acuerdo al alcance de la auditoría y componentes a ser analizados; y materiales necesarios para el desempeño de las actividades de control]

16. Productos a obtener y resultados del examen especial

[Descripción por cada fase de la auditoría los resultados a obtenerse, de acuerdo a la Ley y normativa como la reglamentación para la elaboración de informes y documentos anexos para el trámite de aprobación]

ELABORADO POR

[Nombre y apellido]
Jefe de Equipo

[Nombre y apellido]
Supervisor

REVISADO POR

[Nombre y apellido]
Supervisora General de Calidad

APROBADO POR

[Nombre y apellido]
Director/a [Unidad de Control]

- Anexos
  - Servidores relacionados
  - Matrices de evaluación del control interno y análisis de riesgos
  - Programas de auditoría

ANEXO 6. PROGRAMA DE AUDITORÍA INFORMÁTICA

	PROGRAMA DE AUDITORÍA				
	AUDITORÍA INFORMÁTICA A LA SEGURIDAD DE LA INFORMACIÓN EN LA ENTIDAD XXX				
ENTIDAD:		**COMPONENTES:**			
Nombre de la Entidad XXXX		Gestión de accesos Seguridad física y lógica Continuidad del servicio … …			
CIUDAD: XXX **RESPONSABLE:** AUDITOR OPERATIVO RESPONSABLE		PERÍODO DEL EE: del 1 de enero de 20XX al 31 de diciembre de 20XX			
No.	**OBJETIVOS Y PROCEDIMIENTOS**	**Tiempo estimado (días)**	**Referencia P/T**	**Fecha de ejecución**	**Observación**
	OBJETIVOS:				
1	[DETALLAR LOS OBJETIVOS DE LA AUDITORÍA INFORMÁTICA, CONFORME LA ORDEN DE TRABAJO]				
2	[DETALLAR LOS OBJETIVOS DE LA AUDITORÍA INFORMÁTICA, CONFORME LA ORDEN DE TRABAJO]				
	PROCEDIMIENTOS:				
1	**Gestión de accesos**	**# Días**	**Referencia P/T**	**Fecha de ejecución**	**Observación**
1.1	1.1.1 Verificar si se establecieron procedimientos para la gestión de accesos para la solicitud, revisión, autorización para la administración de cuentas de usuario, estos creación, activación, desactivación y asignación de roles y perfiles. 1.1.2 Identificar el área y personal responsable de la administración de acceso de usuarios 1.1.3 Verificar si se gestionan los accesos de usuarios mediante perfiles y roles asignados conforme las atribuciones y competencias del personal de la Entidad.				
	….				
2	**Seguridad física y lógica**	**# Días**	**Referencia P/T**	**Fecha de ejecución**	**Observación**
2.1	2.1.1 Verificar si se estableció un inventario de activos de información (sistemas, bases de datos, repositorios digitales, servidores, entre otros) y se clasificó conforme su criticidad y sensibilidad de acuerdo a los objetivos institucionales. 2.2.2 Evaluar si se han establecido procedimientos de permanencia y control de accesos del personal interno y externo a la entidad en áreas donde se almacena, procesa y transmite información sensible.				

	2.2.3 Verificar si se cuenta con logs de accesos a servidores de aplicaciones y bases de datos y comunicaciones catalogados como críticos.				
	…				
3	**Continuidad del servicio**	**# Días**	**Referencia P/T**	**Fecha de ejecución**	**Observación**
3.1	3.1.1 Evaluar la cobertura del Plan de Recuperación ante Desastres (DRP). Confirmar que incluya procedimientos detallados para recuperación de sistemas críticos, respaldo de datos y ubicación alternativa de operación.				
	3.1.2 Revisar los resultados de pruebas de simulacros o ejercicios de continuidad. Analizar la frecuencia, alcance y resultados documentados de pruebas de recuperación (simulacros de caída de servicio, pruebas de restauración de backups, entre otros)				
	….				

ANEXO 7. FORMATO PLAN DE PRUEBAS DE AUDITORÍA INFORMÁTICA

CONTRALORÍA GENERAL DEL ESTADO

Dirección Nacional de Auditoría XXXX

Formato Plan de Pruebas de Auditoría Informática
Componente / Elemento/s sobre los cuales se efectuarán el plan de pruebas
(Ejemplo: Externalización / Seguridad de la Información)

OBJETIVO

Redactar de manera clara y precisa qué se pretende verificar o validar durante la auditoría, enfocado en aspectos clave como la seguridad, integridad, disponibilidad y confiabilidad de los sistemas de información

EJEMPLO:
(Evaluar la eficacia de los controles generales de tecnología de la información, especialmente los relacionados con seguridad lógica, gestión de accesos, respaldo de información y continuidad operativa).

ALCANCE

Se describen los límites y el marco general de lo que será evaluado durante la auditoría informática. Define qué sistemas, procesos, períodos de tiempo, ubicaciones y tecnologías se incluirán; también en el alcance debe constar lo que se excluye del análisis de pruebas de ser el caso.

EJEMPLO:
(La evaluación y análisis comprende la Red corporativa (firewall, switches, routers); Servidores de archivos y aplicaciones (Windows Server y Linux); Sistema ERP (SAP); y, Políticas y procedimientos de TI).

CONTROLES A EVALUAR

Comprende el mecanismo o procedimiento específico que la organización ha implementado para mitigar un riesgo significativo relacionado con los componentes y elementos a evaluar; redactarlo correctamente implica describir qué control se analizará, su propósito y cómo contribuye a garantizar la seguridad, integridad o disponibilidad de la información. Para este propósito se elabora una tabla como ejemplo con la siguiente estructura:

Área /Componente	Control evaluado
Seguridad lógica	Control de acceso por usuario/rol
Respaldo	Copias de seguridad automáticas y pruebas de restauración
Continuidad	Existencia y pruebas de plan de contingencia
Cambios	Procedimientos formales para gestión de cambios en sistemas
Actualizaciones	Aplicación de parches de seguridad críticos

MATRIZ DE PRUEBAS

Comprende un instrumento que relaciona los objetivos de la auditoría, los controles a evaluar, los riesgos asociados, los procedimientos de prueba a ejecutar, y la evidencia requerida para sustentar los hallazgos, al respecto se detalla la respectiva matriz de pruebas en función del ejemplo ilustrado en los títulos anteriores del presente documento:

Ítem	Prueba	Objetivo	Técnica / Método	Criterio de éxito
1	Revisión de cuentas de usuario en servidores	Verificar que no existan cuentas inactivas o genéricas activas	Revisión documental + script PowerShell	El 100% de cuentas inactivas deben estar deshabilitadas o eliminadas
2	Verificación de backups	Asegurar que se ejecuten backups completos diarios	Revisión de logs de backup y configuración	Registro de backup con éxito en últimos 7 días
3	Prueba de restauración	Validar que se puede recuperar información respaldada	Simulación con archivos de prueba	Restauración exitosa sin pérdida de datos
4	Validación de parches de seguridad	Verificar si los parches críticos del sistema operativo están aplicados	Revisión de actualizaciones en servidores	100% de parches críticos aplicados en tiempo ≤ 30 días

CRONOGRAMA

El cronograma de pruebas es un elemento clave que permite planificar y organizar de manera eficiente el tiempo y los recursos necesarios para ejecutar los procedimientos de auditoría, especificando fechas, duración estimada, responsables y secuencia de las actividades a realizar; a continuación, un ejemplo:

Actividad	Fecha	Responsable
Revisión documental	17/06/2025	Auditor TI
Pruebas técnicas (scripts, restauraciones)	19/06/2025 20/06/2025	Auditor + Soporte TI
Informe preliminar	21/06/2025	Auditor Líder (Jefe de Equipo)

RECURSOS NECESARIOS

Se describen los recursos pertinentes requeridos para la realización de las pruebas, sean esto humano, materiales, tecnológicos y organizacionales; ejemplos:

Recurso humano:

- Auditor experto en SAP.

Recurso tecnológico:

- Herramientas de auditoría asistida por computadora (CAAT), ACL.

RIESGOS IDENTIFICADOS

Se refieren a las amenazas potenciales que podrían afectar la confiabilidad, seguridad, disponibilidad o integridad de los sistemas y datos auditados. Estos riesgos son fundamentales para enfocar los procedimientos de auditoría en las áreas más críticas y garantizar una evaluación efectiva.

RESULTADO ESPERADO

Comprende un informe del estado de los controles generales de TI, con hallazgos clasificados por criticidad y recomendaciones de mejora.

Versión Documento:	Última Modificación:	Realizado por:
1.0	2025.06.15	Nombre del Auditor de TI

Pruebas para la ejecución de la Auditoría Informática

1. GOBERNANZA Y GESTIÓN DE TI

Evaluar la estrategia y planificación del área, verificando la existencia de un portafolio de proyectos priorizado, indicadores de desempeño, participación del Comité de Gobernanza de TI, modelo organizativo claro, aplicación del código de ética y seguimiento a recomendaciones. Así como las estructuras, normas, políticas y procesos organizacionales, asegurando que la unidad de TI funcione según la estructura aprobada, cuente con procesos documentados, controlados y alineados a la planificación institucional, y se apliquen mecanismos de mejora continua. Finalmente, es fundamental auditar la gestión de riesgos de TI, comprobando la identificación, tratamiento y monitoreo de riesgos, así como la comunicación de los resultados al Comité respectivo para la toma de decisiones y aprobación de requerimientos, y la aplicación de un plan de acción alineado con una matriz de riesgos institucional.

1.1 Estrategia y planificación de TI

1. Evaluar la existencia de un portafolio de proyectos, y si estos se encuentran priorizados y monitoreados.
2. Verificar la existencia y aplicación de indicadores de desempeño, con la finalidad de medir la efectividad de la gestión de TI y monitorear el cumplimiento de metas, objetivos e indicadores; y, las acciones correctivas adoptadas en base a los resultados obtenidos.
3. Evaluar la participación del Comité de Gobernanza de TI en la toma de decisiones.
4. Revisar el modelo de TI, que permita asegurar una estructura definida a través de funciones, roles y responsabilidades. (Ejem.: aplicación de matriz RACI)
5. Comprobar si el código de ética es aplicado en la Entidad, así como, por contratistas y proveedores de TI.
6. Revisar si se efectúan informes al seguimiento y cumplimiento de recomendaciones para la mejora de los procesos de la entidad.

1.2 Estructuras, normas, políticas y procesos institucionales

1. Verificar que la Unidad de TI se encuentra funcionando de acuerdo con la estructura aprobada.
2. Verificar la existencia y funcionamiento de comités de TI a más del Comité de Gobernanza.
3. Verificar que los procesos de TI se encuentren documentados, actualizados, aplicados y controlados.

4. Verificar que los procesos y flujos de información del área de TI se encuentren definidos, formalizados, aplicados, controlados, alineados con la planificación institucional, y cuenten con mecanismos de seguimiento, evaluación y mejora continua a fin de dar cumplimiento a los principios de gobernanza de TI.
5. Evaluar la responsabilidad en la toma de decisiones, la gestión de datos, el uso de recursos tecnológicos y el cumplimiento normativo.
6. Verificar la existencia y aplicación de procedimientos documentados para la gestión de conflictos de interés, y transferencia de conocimiento, con la debida aprobación, y documentación de su aplicación.

1.3 Gestión de los recursos humanos de TI

1. Revisar de las políticas de talento humano relacionadas con TI, su aprobación y actualización.
2. Verificar las definiciones de perfiles y requisitos para los cargos en las áreas de TI.
3. Verificar cumplimiento los requisitos de competencia profesional para TI.
4. Verificar planes de capacitación y desarrollo para el personal de las áreas de TI, y cumplimiento de estos.
5. Verificar las evaluaciones de desempeño al personal que realiza funciones en las áreas de TI.
6. Verificar que los riesgos de segregación de funciones estén considerados.
7. Verificar que se cuente con personal de remplazo para los puestos claves de TI.

1.4 Gestión de riesgos de TI

1. Verificar la existencia de un proceso formal de gestión de riesgo de TI, que sea parte de la gestión de riesgo de la institución.
2. Verificar la asignación de responsabilidades para la gestión de riesgos de TI.
3. Verificar la identificación y tratamiento de los riesgos para los sistemas, infraestructura tecnológica y seguridad de la información.
4. Verificar la existencia de informes periódicos del monitoreo y evaluación de riesgos y su actualización.
5. Verificar los informes de resultados del monitoreo y evaluación de riesgos, y su comunicación al Comité de Gobernanza de TI para la adopción de medidas correctivas.

2. DESARROLLO Y ADQUISICIÓN DE TI

Evaluar el estudio de factibilidad de soluciones tecnológicas, verificando aspectos legales, técnicos, de seguridad, análisis costo-beneficio y riesgos. En el desarrollo y gestión de requisitos, asegurar que existan documentación completa, cumplimiento de requerimientos funcionales y normativos,

participación de las partes interesadas, interoperabilidad, soporte y mantenimiento. En la gestión y control de proyectos, es clave contar con planes aprobados, monitoreo del cronograma, gestión de cambios y cierre formal del proyecto. Para el diseño y desarrollo, verificar la definición adecuada de arquitectura, componentes técnicos y cumplimiento de estándares en la construcción del software, así como la capacitación a usuarios y técnicos. El aseguramiento de la calidad implica revisar que se hayan ejecutado planes de pruebas completos, con documentación de resultados, casos específicos y resolución de problemas. En cuanto a la gestión de configuración, validar la trazabilidad de los cambios, registros actualizados y procedimientos de configuración y versiones. Finalmente, en la adquisición de infraestructura, asegurar que los procesos estén sustentados técnicamente, cumplan normativa vigente, garanticen la compatibilidad e integración con sistemas existentes, y que los bienes estén registrados, documentados y respaldados contractualmente.

2.1 Estudio de factibilidad

1. Verificar la factibilidad legal, mediante la validación de cumplimiento de normativa aplicable a la solución tecnológica, con especial atención a la protección de datos, licenciamiento, contratos, SLAs.
2. Verificar la evaluación de procesos respecto a las nuevas soluciones tecnológicas o cambios propuestos, y su impacto en los procesos actuales.
3. Verificar el análisis de costo beneficio mediante la comparación con otras soluciones de iguales características y sus justificativos.
4. Verificar la identificación y definición de controles de acceso conforme a la normativa gubernamental e institucional, con la finalidad de garantizar la seguridad de los datos.
5. Verificar la matriz de riesgos, de acuerdo con los lineamientos de la entidad y su plan de acción.
6. Verificar la factibilidad técnica que comprende la compatibilidad tecnológica con la arquitectura disponible, servicios de interoperabilidad con la plataforma existente y de requerirlo con otras entidades.
7. Determinar si se puede alcanzar una solución con los sistemas ya existentes, caso contrario, revisar la evaluación de las soluciones alternativas para verificar si éstas cumplen con lo requerido por las partes interesadas.

2.2 Desarrollo y gestión de requisitos

1. Verificar la existencia del procedimiento aprobado y documentación de recolección de las necesidades, que incluya las expectativas, restricciones, interfaces y todos los requisitos funcionales, no funcionales y normativos, para la implementación de los sistemas o aplicativos informáticos.

2. Verificar la existencia de documentación del levantamiento de los requerimientos, como: la aplicación de listas de requerimientos, historias de usuario, casos de uso, diagramas de flujo, etc., definiciones formalizadas por las partes interesadas correspondientes; y, con documentación que evidencie los controles de cambio efectuados.
3. Verificar que los sistemas o aplicativos cumplen con los requerimientos funcionales, y normativas que regulen el proceso automatizado.
4. Revisar la participación de las áreas interesadas en las pruebas de aceptación, recepción y paso a producción de los sistemas o aplicaciones mediante documentación formalizada.
5. Validar el uso de los activos de TI existentes, su reutilización y compatibilidad con la solución tecnológica propuesta.
6. Verificar la implementación de los criterios y condiciones de interoperabilidad con otros sistemas internos y externos.
7. Verificar el cumplimiento de las condiciones de soporte y mantenimiento.
8. Verificar la existencia del registro histórico de versiones.
9. Verificar la ejecución de la migración de datos, en caso de ser requerido.
10. Verificar la existencia y cumplimiento de acuerdos de confidencialidad.
11. Verificar el cumplimiento de los parámetros de rendimiento (tiempo de respuesta), seguridad (cifrado de datos) y disponibilidad, requeridos.

2.3 Gestión y control de proyectos

1. Verificar la existencia de un plan de proyecto aprobado, con la definición de una estructura que supervise el cumplimiento de los objetivos y actividades planteadas, y emita informes periódicos del estado del proyecto, cómo se están gestionando los recursos y sugiera medidas correctivas. (Ejem.: una elevación de costos sustanciales, sobre las cuales la entidad podría recortar ciertas funciones para su reducción)
2. Confirmar que los cambios efectuados al proyecto fueron documentados y aceptados por las partes interesadas.
3. Verificar el monitoreo al cumplimiento del cronograma del proyecto, documentación de los cambios efectuados y su impacto.
4. Verificar la emisión de informes de avance y medidas correctivas para la toma de decisiones.
5. Revisar que se cumplieron las actividades establecidas para el cierre del proyecto, entre ellas la aceptación de los responsables de la realización y aprobación de los productos.

2.4 Diseño/Desarrollo

Diseño de soluciones de software:

1. Verificar que la definición de la arquitectura de datos y componentes estén de acuerdo con la normativa y definición de requerimientos funcionales.

2. Verificar que la definición de la arquitectura incluyó el desglose de los componentes que involucran a más del sistema o aplicativo, software base, bases de datos, lenguajes de programación, infraestructura tecnológica con la capacidad de recursos requeridos.
3. Verificar que se identificaron y describieron las entradas, procesamientos y salidas a través de diseños de pantalla e informes, conforme los requisitos levantados y aprobados para la construcción del sistema o aplicativo informático.
4. Verificar que el diseño y arquitectura, incluyó los servicios externos (Ejem.: interoperabilidad con fuentes externas), análisis de compatibilidad con los servicios tecnológicos existentes, para su integración con la solución tecnológica propuesta.
5. Verificar que la arquitectura, incluyó la definición de las especificaciones técnicas de los equipos, aplicativos de seguridad y servicios de conectividad, entre otros componentes de TI requeridos para el funcionamiento, despliegue y operación de la solución.
6. Verificar que el diseño del software incluyó la escalabilidad entendida como la capacidad de adaptarse a nuevas necesidades, la interoperabilidad para el intercambio y acceso a información con servicios y fuentes externas.
7. Verificar para el caso de adquisición de software, se incluyan cláusulas para la entrega del código fuente y componentes desarrollados por el proveedor, para el uso sin restricciones por parte de la Entidad y como lo estime conveniente.
8. Verificar que la Entidad una vez que el sistema o aplicativo se haya puesto en el ambiente productivo, realizó el registro de la propiedad intelectual y derechos de autor a nombre de la Entidad, ante el organismo competente.

Desarrollo de soluciones de software:

1. Verificar que la construcción de los sistemas o aplicaciones cumplió con los requerimientos funcionales y no funcionales aprobados.
2. Verificar que la codificación y desarrollo de programas y documentos utilizó las metodologías, estándares, procedimientos aprobados, validaciones generales y específicas de aplicación.
3. Verificar que se documentó las modificaciones a los sistemas o aplicativos, y si contribuyeron con correctivos o mejoras.
4. Verificar que se cumplió con las pruebas y procedimientos establecidos para la implantación del nuevo sistema o su actualización, a nivel de seguridades, base de datos, conectividad, configuración; y se documentó el paso a producción.
5. Verificar la capacitación al personal técnico (soporte y mantenimiento).
6. Verificar la documentación de la capacitación a usuarios funcionales en el uso del nuevo sistema, a través de temarios, actas de asistencia y de ser el caso certificados de asistencia y/o aprobación.

2.5 Aseguramiento de la calidad y pruebas

1. Verificar que el plan de pruebas comprenda todas las funcionalidades, responsables y tiempos para su realización.
2. Verificar que la documentación de las pruebas incluya el detalle de la funcionalidad, datos de prueba, reporte de los resultados, responsables de su realización y firmas de responsabilidad.
3. Verificar que las pruebas incluyan la revisión de la normativa y procedimientos relacionados con el alcance y objetivos de la solución, cumplimiento de requerimientos funcionales, no funcionales y seguridad de la información.
4. Verificar que el plan y batería de pruebas incluyan los casos específicos a evaluar, los actores, datos de entrada y resultados esperados, con la documentación de respaldo.
5. Verificar la resolución de los problemas encontrados como resultado de la aplicación de las pruebas.
6. Verificar la existencia de pruebas de integración.
7. Verificar las pruebas de recuperación y de seguridad; con los resultados obtenidos y firmas de responsabilidad de elaboración, revisión y aprobación.

2.6 Gestión de la configuración

1. Verificar que el plan de gestión de la configuración esté alineado con la infraestructura de TI.
2. Validar que el registro o base de datos de configuración contenga información completa y actualizada de los componentes (software, hardware, documentación, versiones, etc.).
3. Contrastar el registro o base de datos de configuración con los activos existentes, a fin de documentar las diferencias detectadas.
4. Verificar la existencia de la trazabilidad y registros de cambios (logs de auditoría), en los procedimientos utilizados para agregar, modificar o eliminar elementos de configuración.
5. Verificar si se aplicó los procedimientos establecidos para la configuración de los sistemas e infraestructura requerida para su puesta en producción, y documentación de los resultados obtenidos.
6. Verificar si se mantienen y respaldan cronológicamente las versiones de los sistemas y configuraciones, de modo tal que la entidad esté en condiciones de volver a versiones conocidas y probadas, si fuese necesario.
7. Verificar la habilitación y temporalidad de los accesos de acuerdo con los roles y responsabilidades requeridos para la administración y funcionamiento de los sistemas de acuerdo con los ambientes de TI.

8. Verificar los informes de auditoría de la configuración, que permita evaluar la aplicación de estándares, políticas y procedimientos establecidos, en los cambios efectuados a la configuración.

2.7 Adquisición de Infraestructura tecnológica

1. Revisar que los requerimientos técnicos y funcionales fueron definidos y documentados con el análisis pertinente de las áreas de TI, funcionales y/o usuarias debidamente suscritas antes de la adquisición.
2. Confirmar que las adquisiciones de soluciones tecnológicas se basen en un análisis de capacidad instalada frente a la capacidad utilizada y se contraste con un análisis de la demanda, que justifique el costo beneficio.
3. Verificar los informes de las tomas físicas de los bienes tecnológicos efectuadas conforme la normativa.
4. Verificar que la entidad contó con los estudios y diseños completos para la adquisición de infraestructura de TI.
5. Verificar que se cumplió con las disposiciones normativas de contratación vigente para la adquisición de la infraestructura de TI.
6. Verificar el análisis de la capacidad del proveedor en relación a la comercialización de infraestructura de TI, autorizado por el fabricante y servicios de mantenimiento y soporte.
7. Verificar que los contratos suscritos incluyen cláusulas sobre niveles de servicio (SLA), soporte, garantías, propiedad intelectual y mantenimiento, este último que garantice la vigencia tecnológica.
8. Verificar que los bienes y/o servicios adquiridos de TI fueron entregados conforme a lo estipulado en las cláusulas contractuales, para lo cual se dejó constancia mediante actas entrega recepción suscritas por los representantes legales de la entidad y del proveedor o sus delegados.
9. Verificar que los bienes y/o servicios adquiridos de TI, se encuentran registrados como activos de la entidad.
10. Verificar que los bienes y/o servicios adquiridos de TI se integraron con los sistemas existentes, a través de pruebas de compatibilidad, rendimiento y seguridad realizadas previo a la puesta en producción.
11. Verificar la existencia de documentación del mantenimiento, renovación y baja de los activos, para los componentes de hardware y software de la infraestructura de TI.

3. OPERACIONES DE TI

El componente de Operaciones de TI se enfoca en evaluar la eficiencia y control de los procesos operativos de tecnología. Incluye la revisión de la gestión de la capacidad, asegurando que los recursos tecnológicos satisfagan la demanda actual y futura; la gestión de cambios, para verificar que existan procedimientos formales que minimicen riesgos y aseguren la trazabilidad de las modificaciones; y la gestión del personal de TI, evaluando la asignación de funciones, competencias y cumplimiento de normativas laborales y éticas.

También se analiza la gestión de incidentes y problemas, para confirmar la existencia de mecanismos efectivos de registro, atención y solución oportuna. La gestión de niveles de servicio revisa la existencia y cumplimiento de acuerdos (SLAs) con usuarios y proveedores, y la gestión de activos a través del control del inventario tecnológico, su uso adecuado y mantenimiento actualizado.

3.1 Gestión de la Capacidad

1. Verificar reportes de monitoreo periódico del rendimiento de los sistemas y recursos tecnológicos para detectar cuellos de botella o sobrecargas.
2. Verificar la existencia de documentación que permita identificar, analizar y resolver problemas relacionados con la falta de disponibilidad o insuficiencia de recursos.
3. Constatar que en los casos donde la capacidad esté sujeta a servicios provistos por terceros, se cumplieron los acuerdos contractuales y se verificó periódicamente que la capacidad contratada corresponda con la demanda real, permitiendo ajustes correctivos oportunos.
4. Revisión del acuerdo o la guía de funcionamiento que el grupo de TI está utilizando.
5. Comparación del desempeño real del servicio con los parámetros de referencia establecidos.

3.2 Gestión de Cambios

1. Verificar la existencia de procedimientos de gestión de cambios debidamente aprobados.
2. Verificar que todos los cambios propuestos hayan sido evaluados considerando su impacto técnico, operativo, de seguridad de la información y de cumplimiento normativo, priorizados y aprobados en función de su importancia, impacto y urgencia.
3. Verificar que se realizaron pruebas antes de la implementación de los cambios en ambientes controlados previo a su paso a producción.
4. Verificar que exista el análisis de compatibilidad con otros sistemas para evitar reversiones.
5. Verificar que se mantienen planes de respaldo antes del paso a producción y de reversión (Rollback), en caso de que el cambio falle.
6. Comprobar que se realiza una implementación controlada de cambios, de forma estructurada y programada, fuera de horarios críticos para no impactar a la continuidad de los sistemas y servicios.
7. Verificar que existan mecanismos de monitoreo posteriores a la implementación de los cambios, con el fin de detectar oportunamente posibles incidentes, y evaluar si se alcanzaron los resultados esperados.
8. Verificar la documentación de cambios de emergencia que se han realizado durante el período auditado, y los resultados obtenidos.

3.3 Gestión de Incidentes y problemas

1. Constatar la clasificación y priorización de incidentes y problemas, que permitan determinar el impacto, urgencia y prioridad para la resolución oportuna.
2. Verificar informes del análisis técnico para gestionar incidentes y problemas recurrentes, de ser el caso permita escalar a otras instancias.
3. Revisar los procedimientos de la mesa de servicio a fin de verificar si se han definido e implementado mecanismos de escalamiento para los incidentes que no pueden ser resueltos de forma inmediata, conforme los criterios establecidos en el Acuerdo de Nivel de Servicio (SLA).
4. Verificar que existan mecanismos para la gestión de incidentes y problemas.
5. Verificar si se identificó la fuente del incidente. Verificar las medidas adoptadas (procedimiento de cambio, amonestación, capacitación, etc.).

3.4 Gestión de Servicios

1. Comprobar que se mantiene un listado o catálogo completo y actualizado de los servicios TI.
2. Verificar que se cuente con registros para la gestión de los servicios, considerados en el listado o catálogo.
3. Verificar los informes de cumplimiento de SLA, OLA y UC confirmar si todos los indicadores fueron revisados y sus resultados y recomendaciones comunicados a las instancias correspondientes.
4. Verificar que los servicios de TI definidos por la entidad están cubiertos por un SLA, debidamente suscrito, si se gestionan indicadores, tiempos de atención y resolución, si se incluyen parámetros como disponibilidad, soporte, capacidad, continuidad y si está claramente establecido quién provee, quién consume y quién supervisa el servicio.
5. Verificar que en el SLA se han establecido sanciones, compensaciones o planes de mejora y se han aplicado de ser el caso.
6. Verificar que los SLA se revisan regularmente para ajustarse a las necesidades institucionales.
7. Verificar que se realice encuestas o reuniones con los usuarios finales para evaluar la satisfacción respecto a los niveles de servicio.

3.5 Gestión de Activos de TI

1. Verificar documentación del detalle del ciclo de vida de los activos.
2. Verificar que los activos estén clasificados por tipo, criticidad o nivel de confidencialidad, y que cuenten con identificadores únicos (etiquetado), para facilitar su control, rastreo y protección.
3. Verificar reportes de mantenimiento y soporte a equipos de TI.

4. Verificar que cada activo tenga un custodio designado formalmente, a través de actas o su similar para la entrega-recepción.
5. Constatar informes de verificaciones periódicas de activos, con el propósito de mantener actualizados su estado y ubicación lo que permitirá asegurar la actualización del inventario de los activos y su registro contable.
6. Verificar la gestión de licencias de software, con la determinación del estado de las licencias (válidas / caducadas) e informes con los riesgos identificados de carácter legal, seguridad de la información u otros.
7. Verificar el registro de contratos de adquisición, mantenimiento, soporte, y garantías, que cumplan con obligaciones legales.
8. Verificar las disposiciones que garantizan que los datos son eliminados antes de la remoción o reutilización de los equipos.

4. EXTERNALIZACIÓN

Evaluar que la entidad gestione adecuadamente los servicios tecnológicos contratados a terceros. Esto implica verificar la existencia de un análisis previo que justifique la externalización, la formalización de contratos con cláusulas claras sobre niveles de servicio, seguridad, confidencialidad y cumplimiento normativo. También revisar que haya mecanismos de supervisión y evaluación del desempeño de los proveedores y control de vulnerabilidades, así como evidencia de seguimiento, mitigación de riesgos y aplicación de medidas correctivas en caso de incumplimientos. Además, es importante comprobar que la externalización no comprometa la continuidad operativa, ni la integridad y confidencialidad de la información.

4.1 Cumplimiento legal y normativo

1. Validar que la política o procedimiento de externalización de servicios de TI, sea actualizada, aprobada y esté alineada con los principios de gobernanza de TI y los objetivos estratégicos de la entidad.
2. Revisar que la política o procedimiento haya sido difundida a las áreas relacionadas con los servicios externalizados (TI, jurídico, adquisiciones y procesos de la entidad que dan uso a los servicios).
3. Verificar que los contratos de bienes y servicios externalizados cumplieron con las cláusulas y normativa de contratación pública, protección de datos personales, confidencialidad y responsabilidad.
4. Revisar los informes y registros de monitoreo y seguimiento de los servicios prestados por el proveedor en cuanto al cumplimiento de lo establecido en el contrato y acuerdo de nivel de servicio.
5. Verificar que los contratos y acuerdos de nivel de servicio (SLA), hayan sido suscritos por la máxima autoridad de la entidad o su delegado y el representante legal del proveedor.
6. Verificar la existencia de indicadores de desempeño y métricas de calidad; y la descripción de los parámetros de medición del servicio.

7. Revisión del acuerdo de confidencialidad para verificar que toda la información relevante esté resguardada.
8. Verificar que los procesos, datos y software estén bajo control de la entidad.
9. Validar que el personal reciba el traspaso de conocimientos de los bienes y/o servicios contratados durante la vigencia del contrato.
10. Verificar la existencia de acuerdo sobre la propiedad de los datos y de las aplicaciones para el soporte de las operaciones de la entidad, así como la devolución en tiempo y forma de estos al finalizar los servicios y, garantías para la migración de los servicios, aplicaciones y datos, y posterior eliminación segura en las plataformas del proveedor.

    En el caso de servicios en la nube verificar:

11. Que el SLA incluya la definición de medidas de desempeño como: nivel de servicio, nivel de capacidad (ejem: número máximo de usuarios), tiempos de respuesta (ejem: rapidez en una transacción).
12. La existencia de acceso a sus datos y redes alojados por el proveedor, especialmente al concluir el contrato.
13. Que el proveedor realice el monitoreo del servicio en la nube y que estas sean verificadas por la entidad.
14. Control de acceso a los servicios e información.

5. GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO

Realizar pruebas para verificar que la entidad cuente con un plan de continuidad operativa (BCP) y un plan de recuperación ante desastres (DRP) formalmente aprobados, actualizados y alineados con los riesgos identificados. Comprobar la existencia de análisis de impacto al negocio (BIA), así como de estrategias documentadas para la recuperación de sistemas críticos. Además, es necesario revisar si se han realizado pruebas periódicas de simulación o validación de dichos planes, con resultados documentados y acciones de mejora. También confirmar que las responsabilidades estén claramente asignadas, que el personal clave haya sido capacitado y que exista un procedimiento definido para la activación de los planes ante eventos disruptivos.

5.1 Política, plan y organización para la continuidad del negocio

1. Verificar que en la política o procedimiento se hayan definido los compromisos para asegurar la disponibilidad de los servicios críticos de TI ante interrupciones o fallos, el alcance, objetivos, roles y responsables y gestión de riesgos.
2. Verificar que la política o procedimiento fue difundido.

3. Verificar que el plan de continuidad del negocio (BCP), esté alineado con los requisitos del negocio y los riesgos identificados.
4. Verificar que el plan de continuidad del negocio incluyó la planificación de contingencias, procedimientos para la respuesta frente a emergencias, recuperación de usuarios y actividades de gestión de crisis.
5. Evaluar que el plan de continuidad del negocio cubra todos los recursos de TI con la identificación de los sistemas y servicios considerados como críticos para la entidad.
6. Revisar los resultados de las pruebas y acciones correctivas derivadas; y que el plan de continuidad haya sido actualizado e informadas a las autoridades para su seguimiento.
7. Verificar que existan los procedimientos de evaluación y estrategias de recuperación para cada sistema o aplicativo en específico.
8. Confirmar la existencia del Análisis de Impacto al Negocio (BIA) ante amenazas (cortes de energía, ataques ransomware, incendios, etc.) y la evaluación del riesgo.
9. Verificar que el plan de recuperación ante desastres cuente con la descripción de las actividades de la infraestructura que soportan los servicios de TI, que entre otros aspectos contenga:
   - Procedimientos para restaurar sistemas, datos y servicios tecnológicos en caso de interrupción.
   - Medios o estrategias de recuperación de la infraestructura de TI y sus servicios.
   - Roles y responsabilidades para la aplicación
10. Verificar que el plan de recuperación ante desastres fue comunicado al personal de las áreas técnicas y funcionales.
11. Verificar que para el plan de respaldo y restauración se han definido políticas, procedimientos y herramientas para realizar copias de seguridad de los datos, configuraciones y sistemas de acuerdo con su criticidad, así como su restauración en caso de pérdida, daño o desastre, que sean compatibles con los requisitos de tolerancia establecidos en el BCP.
12. Verificar que, en el Plan de respaldo y restauración, se definieron roles y responsabilidades para su aplicación, así como hardware, datos y software.
13. Verificar que, en el Plan de respaldo y restauración, se definieron y aplicaron los procedimientos que incluyan mecanismos de cifrado, control de acceso a los respaldos y ubicación.
14. Verificar que, el Plan de contingencia, cuenta con la definición de roles y responsabilidades, y acciones para prevenir, responder y recuperarse de incidentes que afecten la operación de los sistemas, servicios y recursos de TI.
15. Verificar para el Plan de contingencia, el análisis de riesgos, estrategias de continuidad (frecuencia de respaldos, sitios alternos o de recuperación, contratos con proveedores externos para recuperación rápida, redundancia, seguridad perimetral).

6. SEGURIDAD DE LA INFORMACIÓN

Evaluar los mecanismos implementados para proteger la confidencialidad, integridad y disponibilidad de la información institucional. Esto incluye verificar la existencia y aplicación de una política de seguridad formal, la definición clara de roles y responsabilidades en la organización de la seguridad de TI, y el control adecuado sobre los activos de información. También se debe revisar la efectividad de las medidas de seguridad física y del entorno, los controles implementados para el acceso lógico y físico a los sistemas, y los procedimientos establecidos para la gestión de incidentes de seguridad, incluyendo su registro, análisis, respuesta y mejora continua.

6.1 Evaluación de Riesgos de Seguridad de la Información

1. Verificar que la entidad cuenta con un proceso formalizado para la evaluación de riesgos de seguridad de la información.
2. Verificar que la entidad ha aplicado el proceso de evaluación de riesgos de seguridad de la información.
3. Verificar que los riesgos de seguridad de la información, ciberseguridad, continuidad del negocio y privacidad se encuentran integrados al mapa de riesgos de TI.

6.2 Política de Seguridad de la Información

1. Verificar que la política esté alineada con los objetivos estratégicos de la organización y con el Esquema Gubernamental de Seguridad de la Información u otra normativa en el ámbito de seguridad vigente.
2. Verificar que la política refiera leyes, reglamentos y estándares que las instituciones deberían cumplir como protección de datos personales, ciberseguridad, contratos, etc.
3. Verificar la privacidad y consentimiento en el tratamiento de datos personales.
4. Verificar que se respete la privacidad y consentimiento en el tratamiento de datos personales.
5. Verificar que existe el plan de seguridad de TI en el que conste: Roles y responsabilidades, concientización y capacitación a los usuarios en seguridad.

6.3 Organización de la Seguridad de TI

1. Verificar que las designaciones de los roles y funciones del comité de seguridad de la información fueron comunicados a sus responsables para su cumplimiento.
2. Verificar la existencia de documentación de reuniones de coordinación entre las demás unidades y las áreas de TI, y que los temas tratados y

acuerdos consten en las actas correspondientes debidamente formalizadas.
3. Validar que los contratos y acciones de personal de los funcionarios incluyan cláusulas sobre deberes y responsabilidades en seguridad de la información.
4. Revisar la existencia de procedimientos para la incorporación de requisitos de seguridad en el desarrollo de software o adquisición de sistemas, infraestructura de TI y servicios.

6.4 Gestión de Activos de Información

1. Verificar la existencia de un inventario actualizado de activos de información (hardware, software, datos, servicios), con la inclusión de la identificación y custodio asignado.
2. Verificar que los inventarios de activos de TI se encuentren documentados y actualizados, en los que se identifique información de su procedencia, actividades de mantenimiento y estado de funcionamiento.
3. Verificar la existencia de la clasificación de activos, considerando su nivel de criticidad, confidencialidad, integridad y disponibilidad.
4. Revisar la existencia y difusión de políticas de uso de activos (Ejem.: uso de equipos, acceso a Internet, uso de dispositivos móviles).
5. Verificar la existencia y funcionamiento de controles implementados para la protección de activos utilizados fuera del entorno de la entidad (teletrabajo, dispositivos móviles).
6. Verificar que la entidad disponga de software instalado debidamente licenciado.
7. Revisar bitácoras o registros de ingreso/salida de activos (como laptops, dispositivos externos), a fin de validar la trazabilidad y autorización de los movimientos realizados.

6.5 Seguridad física y del entorno

1. Verificar la existencia de políticas o procedimientos de seguridad física y del entorno.
2. Verificar que las políticas o procedimientos contengan actividades para: control de acceso físico; protección ambiental; resguardo de instalaciones críticas (CPDs, data centers).
3. Comprobar la existencia de cerraduras, cámaras de vigilancia, alarmas; detectores de humo, extintores, sistemas contra incendios; UPS, generadores, y sistemas de respaldo energético, etc.
4. Verificar la existencia y mantenimiento de: aires acondicionados/climatización de sala de servidores, control de humedad y temperatura, sistemas de detección y extinción de incendios.
5. Revisar la existencia de un Plan de Evacuación y Respuesta ante Emergencias.

6. Verificar que se realizó simulacros y capacitaciones al personal.
7. Confirmar que las copias de seguridad se almacenan en ubicaciones seguras y que éstas tengan controles de acceso y ambientales adecuados.
8. Revisar que existan logs de acceso físico y reportes de incidentes.
9. Verificar el análisis posterior a incidentes (robo, acceso no autorizado, daño físico).

6.6 Control de accesos

1. Evaluar que se definieron criterios de asignación de permisos; Niveles de acceso por rol; Acceso mínimo necesario (principio de menor privilegio); Autenticación y autorización; Accesos remotos.
2. Verificar que las cuentas activas correspondan a usuarios autorizados y con los privilegios adecuados.
3. Verificar logs o reportes de TI con la desactivación oportuna de cuentas tras la salida de personal.
4. Validar que se sigan procedimientos formales para gestionar los accesos.
5. Evaluar la seguridad de los mecanismos de acceso.
6. Verificar que los accesos con privilegios elevados estén controlados y monitoreados.
7. Evaluar que se revisen regularmente los accesos asignados.
8. Validar el registro y monitoreo de intentos de acceso y uso del sistema.
9. Verificar que se cumplan los requisitos establecidos en las políticas de contraseñas en todas las plataformas tecnológicas.

6.7 Gestión de incidentes y acontecimientos relacionados con seguridad de TI

1. Comprobar si la organización responde adecuadamente a incidentes.
2. Evaluar la trazabilidad y seguimiento de incidentes históricos.
3. Validar que los incidentes se gestionan según su impacto y urgencia.
4. Verificar la existencia de monitoreo automatizado de seguridad.
5. Comprobar que existe un equipo definido para atender incidentes de seguridad.
6. Comprobar que los incidentes generan acciones de mejora.
7. Verificar que existen mecanismos para el reporte de incidentes.

6.8. Seguridad de la información ligada al personal

En adicional al contenido en el elemento "Gestión de los recursos humanos de TI" del componente "Gobernanza y Gestión de TI", se deberían considerar los siguientes ítems de evaluación:

1. Verificar el establecimiento de programas de concientización, educación y formación específica en materia de seguridad de la información
2. Verificar la realización de la concientización, educación y formación en materia específica de seguridad de forma periódica al personal.
3. Verificar que la entidad prepara y pone en práctica un plan de formación adecuado para los roles claves que gestionan seguridad TI.

7. CONTROLES DE APLICACIÓN

El componente de Controles de Aplicación se enfoca en evaluar la confiabilidad, integridad y seguridad de las funciones automatizadas dentro de los sistemas. Las pruebas deben verificar la existencia de controles sobre los datos de entrada, asegurando su validez, integridad y autorización antes del procesamiento; controles de procesamiento, que garanticen la correcta ejecución de las operaciones conforme a las reglas del negocio; y controles sobre los datos de salida, asegurando la exactitud, confidencialidad y distribución adecuada de la información generada. Además, se deben revisar los controles de seguridad de las aplicaciones, incluyendo restricciones de acceso, trazabilidad de acciones, y medidas que prevengan modificaciones no autorizadas al código o a los datos procesados.

7.1 Controles de datos de entrada

1. Verificar que existan validaciones automáticas para campos obligatorios, formatos y rangos de valores, antes de su ingreso al sistema.
2. Evaluar la existencia de controles para prevenir la duplicación de registros o datos clave.
3. Confirmar que los usuarios tengan roles o permisos claramente definidos para el ingreso de datos.
4. Verificar si las modificaciones a los datos ingresados quedan registradas en bitácoras o logs.
5. Comprobar la existencia de procedimientos documentados para preparar y validar la información fuente.

7.2 Controles de procesamiento

1. Verificar que el sistema realiza los cálculos y operaciones conforme a reglas de negocio documentadas.
2. Revisar la existencia de mecanismos de control como totales de verificación o hash total.
3. Confirmar si las transacciones procesadas quedan registradas en bitácoras de auditoría.
4. Evaluar que el procesamiento sea automático y sus resultados sean consistentes.

5. Analizar que se implementó controles de integridad durante todo el ciclo de procesamiento.
6. Revisar la existencia de alertas automáticas en caso de errores de procesamiento.
7. Comprobar la existencia de revisiones funcionales y técnicas de la lógica implementada en el sistema.
8. Evaluar el tratamiento de excepciones durante el procesamiento de transacciones críticas.

7.3 Controles de los datos de salida

1. Verificar que los reportes generados por el sistema reflejen fielmente los datos procesados.
2. Confirmar que los reportes sean completos, precisos y generados de forma oportuna.
3. Evaluar que existan mecanismos para revisar y aprobar reportes antes de su distribución.
4. Revisar que los reportes contengan controles como sumas de verificación o numeración de páginas.
5. Comprobar que la distribución de los reportes está controlada y documentada.
6. Verificar que existan procedimientos para conciliar datos de entrada y salida.
7. Confirmar que los reportes con información sensible tengan restricciones de acceso.

7.4 Controles de seguridad de aplicaciones

1. Verificar que existan perfiles de acceso claramente definidos y documentados.
2. Revisar que se aplican mecanismos de autenticación y autorización.
3. Evaluar que los datos están protegidos en tránsito y en reposo mediante cifrado u otros medios.
4. Comprobar la existencia de registros de accesos y su monitoreo periódico.
5. Verificar que exista segregación de funciones en operaciones críticas.
6. Evaluar que los cambios en permisos de acceso estén debidamente autorizados.
7. Revisar que el sistema incluya mecanismos para detectar e informar incidentes de seguridad.
8. Confirmar la existencia de revisiones periódicas sobre los accesos a la aplicación.

ANEXO 9. HOJA DE HALLAZGO

HOJA DE HALLAZGO

Auditoría Informática .....

Componente:	
Subcomponente:	

TÍTULO DEL COMENTARIO:

CONDICIÓN:

	REF. PT

CRITERIO:

CAUSA(s):

NOMBRES DE SERVIDORES / PERSONAS Y PERÍODO DE GESTIÓN:

EFECTO:

OPINIONES DE LA ENTIDAD O PUNTOS DE VISTA DE LOS VINCULADOS

CRITERIO DE AUDITORÍA SOBRE PUNTOS DE VISTA:

Respuestas a la Comunicación de Resultados Provisionales:

Respuestas Posterior a la Conferencia Final:

CONCLUSIÓN:

RECOMENDACIONES:

Elaborado por: XXX Firma: _____

Revisado por: XXX Firma: _____

Supervisado por: XXX Firma: _____

Fecha:

ANEXO 2

GUÍA TÉCNICA PARA LA REALIZACIÓN DE AUDITORÍAS INFORMÁTICAS

JUNIO - 2025

ÍNDICE

1. INTRODUCCIÓN

1.1. PROPÓSITO DE LA GUÍA
1.2. OBJETIVOS
1.2.1. Objetivo General
1.2.2. Objetivos Específicos
1.3. AUDIENCIA DESTINATARIA Y PERFILES DE USO

2. ALCANCE Y ÁMBITO DE APLICACIÓN

2.1. ALCANCE DE LA GUÍA
2.2. ÁMBITO DE APLICACIÓN
2.3. HABILITADORES DE GOBIERNO Y GESTIÓN DE TI
2.4. COMPONENTES DE ANÁLISIS EN LA AUDITORÍA INFORMÁTICA
2.4.1. Gobernanza y Gestión de TI
2.4.2. Desarrollo y Adquisición de TI
2.4.3. Operaciones de TI
2.4.4. Externalización
2.4.5. Gestión de la Continuidad del Negocio
2.4.6. Seguridad de la Información
2.4.7. Controles de Aplicación

3. LIMITACIONES Y EXCLUSIONES

3.1. LIMITACIONES
3.2. EXCLUSIONES

4. MODELO DE MADUREZ DE TI

4.1. MARCO DE REFERENCIA
4.2. NIVEL DE CAPACIDAD
4.3. CLAVES PARA LA EVALUACIÓN
4.4. CALIFICACIÓN DE LA ENTIDAD

5. PRUEBAS DE AUDITORÍA DE TI

ACRÓNIMOS

GLOSARIO DE TÉRMINOS

ANEXOS

1. INTRODUCCIÓN

La Contraloría General del Estado (CGE), como Entidad Fiscalizadora Superior (EFS) tiene entre sus facultades efectuar el control de los recursos informáticos de las entidades, organismos del sector público y de las personas jurídicas de derecho privado que dispongan de recursos públicos para evaluar su eficiencia y efectividad.

Las entidades gubernamentales han adoptado cada vez más las tecnologías de la información y la comunicación (TIC) para llevar a cabo sus funciones y ofrecer diversos servicios; tales sistemas basados en las TIC son comúnmente conocidos como Sistemas de Información (SI) o Sistemas de Tecnología de la Información (TI).

El desarrollo continuo de la tecnología de la información y la comunicación ha hecho posible capturar, almacenar, procesar y entregar información en forma electrónica; esta transición hacia el procesamiento electrónico ha provocado un cambio significativo en el entorno en el que debería responder la CGE; por otra parte, el gasto del gobierno en TI está en aumento, por lo tanto, se hace imperativo para la CGE desarrollar la capacidad adecuada para llevar a cabo las auditorías informáticas.

La rápida migración a plataformas digitales y servicios en la nube amplía la superficie de riesgo y exige que la CGE adapte sus métodos a marcos internacionales y a la normativa nacional, con el fin de verificar que las entidades mantengan niveles de madurez adecuados en gobierno y gestión de TI, protejan los datos y garanticen la continuidad de los servicios.

En las auditorías informáticas se examinarán y verificarán los sistemas, las aplicaciones, infraestructura y procesos de tecnología de la información, entre otros componentes para identificar y corregir vulnerabilidades, incumplimientos y riesgos que puedan afectar a la integridad, la confidencialidad, la

disponibilidad de la información y los recursos informáticos, a fin de reducir el impacto en la prestación de los servicios y en consecuencia la misión de la entidad.

La auditoría informática debería enfocarse en generar valor público, evaluando si la tecnología mejora la transparencia, la eficiencia y el cumplimiento legal, de modo que el uso de recursos públicos se traduzca en servicios confiables y oportunos para la ciudadanía, y en una rendición de cuentas efectiva.

1.1. PROPÓSITO DE LA GUÍA

Establecer orientación a los equipos de la Contraloría General del Estado (CGE) en la evaluación de controles y realización de pruebas durante la ejecución de las órdenes de trabajo; la Guía busca garantizar independencia, aplicación técnica y generación de valor público como resultado de la realización de auditorías informáticas a los componentes de las tecnologías de la información.

1.2. OBJETIVOS

1.2.1. Objetivo General

Estandarizar la ejecución de las pruebas para los procedimientos de auditorías de TI, mediante la sistematización de técnicas aplicables a diversos contextos y ámbitos de aplicación de los componentes objeto de evaluación; esto proporciona a los auditores una ruta clara de trabajo que facilite la práctica de acuerdo con las normas generales y específicas, estándares internacionales, así como del marco legal aplicable, garantizando una función de control con altos estándares profesionales.

1.2.2. Objetivos Específicos

- Garantizar la aplicación de lo establecido en el Manual de Auditoría Informática para la evaluación tanto de los sistemas de información como de la infraestructura y los servicios que los soporta.
- Describir los procedimientos técnicos que respalden las actividades de control.
- Planificar la ejecución de pruebas de cumplimiento y pruebas sustantivas para responder a los objetivos de control establecidos en los programas de auditoría.
- Evaluar los controles clave de los procesos y sistemas de información que respaldan los objetivos institucionales.

1.3. AUDIENCIA DESTINATARIA Y PERFILES DE USO

Esta Guía está destinada a los Auditores de la Contraloría General del Estado que realizan auditorías informáticas, o participan en apoyo a otras auditorías de cumplimiento, desempeño y financieras que requieren el análisis puntual de componentes tecnológicos.

La Guía también puede servir de referencia secundaria a órganos de control interno de las entidades públicas, a fin de alinear sus propias prácticas con los componentes objeto de evaluación por la CGE, en las acciones de control que lleva a cabo.

2. ALCANCE Y ÁMBITO DE APLICACIÓN

2.1. ALCANCE DE LA GUÍA

Tendrá como alcance la aplicación práctica para la realización de los exámenes planificados o imprevistos, establecidos en el Plan Anual de Control, y de cualquier acción de control que sea requerida por la CGE; en la que se demande revisiones de componentes de gobierno y gestión de las tecnologías de la información conforme a lo descrito en el Manual de Auditoría Informática; no está dentro del alcance formular procedimientos específicos de pruebas a controles.

2.2. ÁMBITO DE APLICACIÓN

De acuerdo con lo establecido en el Manual de Auditoría Informática, los ámbitos de aplicación de la auditoría informática permiten orientar los esfuerzos de control y evaluación en el área de tecnologías de la información, facilitando la planificación según riesgos, prioridades institucionales y objetivos de gestión; estos ámbitos se clasifican en cinco grandes categorías:

- Gestión Informática, donde se evalúa el alineamiento de la gestión de TI con los objetivos estratégicos institucionales, y se revisa la gobernanza de TI, gestión de riesgos, planificación estratégica, uso de recursos, contratación de servicios y calidad del servicio entregado.

- Seguridad de TI, en la que se analizan las acciones preventivas, correctivas y detectivas para proteger los activos de información, y se examinan las políticas de seguridad, gestión de accesos, cifrado, incidentes, respaldos, antivirus y controles de acceso.

- Infraestructura Tecnológica, donde se evalúa la arquitectura tecnológica (servidores, redes, centros de datos, etc.), y, además, se verifica la existencia y operatividad de planes de continuidad del negocio (BCP) y recuperación ante desastres (DRP), así como respaldos y centros alternos.

- Sistemas o Aplicativos, en la que se revisa la funcionalidad, integridad, seguridad y eficiencia de los sistemas de información, y se evalúa el diseño, desarrollo, implementación, operación y mantenimiento de los aplicativos, incluyendo trazabilidad, documentación, control de cambios y calidad del código fuente.

- Adquisiciones Tecnológicas, donde se examina la legalidad, pertinencia y eficiencia de las contrataciones de TIC, y se revisa desde la planificación hasta la implementación y uso de los recursos tecnológicos, asegurando el cumplimiento normativo y la alineación con las necesidades institucionales.

2.3. HABILITADORES DE GOBIERNO Y GESTIÓN DE TI

Para satisfacer los objetivos institucionales, cada entidad necesita establecer, personalizar y sostener un sistema de gobierno y gestión creado a partir de una serie de habilitadores transversales en la organización; estos habilitadores son factores que, de forma individual y colectiva, contribuyen al buen funcionamiento del sistema de gobierno de la institución en cuanto a TI.

Los habilitadores pueden ser de diversos tipos; los más comunes son los procesos; sin embargo, los habilitadores de un sistema de gobierno incluyen también estructuras organizativas, políticas y procedimientos, elementos de información, cultura y comportamiento, habilidades y competencias, y servicios, infraestructura y aplicaciones.

Habilitadores de un Sistema de Gobierno

FUENTE: Adaptado de Cobit 2019 (ISACA)

I. Los Procesos: describen una serie de prácticas y actividades organizadas para lograr determinados objetivos y producir una serie de salidas que contribuyan a la consecución de la totalidad de los objetivos relacionados con las TI.

II. Las Estructuras organizativas: son las entidades claves de toma de decisiones en una institución.

III. Los Principios, Políticas y Marcos de referencia: son aquellas que convierten el comportamiento deseado en una aplicación práctica para la gestión diaria.

IV. La Información: incluye toda la información producida, comunicada y utilizada por la institución; el marco se centra en la información y en la comunicación requerida para el funcionamiento eficaz del sistema de gobierno de la institución.

V. La Cultura, Ética y Comportamiento de individuos y de la institución: Es la cultura organizacional, la cual juega un papel crucial en el éxito del control interno, ya que una cultura ética fuerte puede disuadir comportamientos no deseados y fomentar la integridad.

VI. Las Personas, habilidades y competencias: aquellas que son necesarias para tomar buenas decisiones, ejecutar medidas correctivas y completar satisfactoriamente todas las actividades.

VII. Los Servicios, infraestructura y aplicaciones: incluyen la infraestructura, la tecnología y las aplicaciones que brindan a la institución un sistema de gobierno para el procesamiento de I&T.

Los habilitadores de cualquier tipo pueden ser genéricos o variantes de los componentes genéricos; por lo general en las prácticas de auditoria se combinan elementos que se encuentran de en varios componentes para dar una visión 360 en las revisiones y evaluaciones.

A continuación, se muestran los habilitadores de gobierno y gestión, y se listan aquellas normas de control interno (NCI) que consideran de alguna manera aspectos de estos habilitadores.

Habilitadores del MGGTI	Normas de Control Interno (NCI) - Ecuador
I. Procesos	100-01, 100-02, 100-04, 200-02, 200-07, 200-08, 300-01, 300-02, 300-03, 300-04, 401-01, 401-02, 401-03, 401-04, 401-05, 407-01, 407-03, 407-05, 407-08, 407-09, 410-01, 410-03, 410-04, 410-07, 410-08, 410-09, 410-10, 410-11, 410-12, 410-13, 410-14, 410-17, 500-01, 500-02, 600-01, 600-02
II. Estructura organizativa	100-01, 100-02, 100-03, 100-04, 200-02, 200-04, 200-05, 200-06, 200-07, 200-09, 401-01, 401-04, 407-02, 407-03, 410-01, 410-02, 410-03
III. Flujos y elementos de información	200-02, 300-01, 300-02, 401-05, 407-10, 410-04, 410-06, 500-01, 500-02, 600-01
IV. Personas, habilidades y competencias	100-03, 200-01, 200-03, 200-05, 200-06, 401-04, 407-01, 407-02, 407-03, 407-04, 407-05, 407-06, 407-07, 407-08, 407-09, 407-10, 410-16

Habilitadores del MGGTI	Normas de Control Interno (NCI) - Ecuador
V. Políticas y procedimientos	100-01, 100-02, 200-01, 200-03, 200-08, 300-03, 300-04, 401-01, 401-02, 401-05, 407-06, 407-07, 410-03, 410-05, 410-06, 410-10, 410-11, 410-12, 410-13, 410-17
VI. Cultura, ética y comportamiento	100-01, 100-04, 200-01, 200-08, 407-08
VII. Servicios, infraestructura y aplicaciones	410-04, 410-05, 410-06, 410-07, 410-08, 410-09, 410-10, 410-11, 410-12, 410-13, 410-14, 410-15, 410-16, 410-17, 500-01, 500-02

Fuente: Elaboración propia

Nota: Estas normas son de aplicación obligatoria para las entidades sujetas a fiscalización; y es un requisito de competencia profesional que estas normas deberían formar parte del conocimiento de los auditores para que por medio de la auditoría se pueda revisar y evaluar su cumplimiento de parte de las entidades sujetas de fiscalización.

2.4. COMPONENTES DE ANÁLISIS EN LA AUDITORÍA INFORMÁTICA

La definición de los componentes de la auditoría informática establece claramente el alcance, guía el análisis técnico y optimiza el uso de recursos, asegurando un proceso de auditoría ordenado y completo; conforme a lo establecido en el Manual de Auditoría Informática, estos componentes son los siguientes:

2.4.1. Gobernanza y Gestión de TI

La Gobernanza y Gestión de TI establece el marco que guía las operaciones tecnológicas para alinear los sistemas de TI con los objetivos estratégicos, optimizar recursos y controlar riesgos. En auditoría informática, su análisis evalúa cómo la gestión tecnológica satisface las necesidades de las partes interesadas y contribuye al logro institucional.

2.4.2. Desarrollo y Adquisición de TI

El Desarrollo y Adquisición de TI abarca la creación de sistemas y la compra de tecnología (hardware, software y servicios) para cubrir necesidades institucionales, mejorar la eficiencia y fortalecer la competitividad, según los recursos y objetivos de cada organización.

2.4.3. Operaciones de TI

Las Operaciones de TI abarcan las actividades, procedimientos y controles para administrar y mantener la infraestructura tecnológica, asegurando la disponibilidad de sistemas, la gestión de incidentes, el control de cambios y el monitoreo del rendimiento de los servicios.

2.4.4. Externalización

La externalización (outsourcing, tercerización), consiste en contratar a un proveedor externo para gestionar total o parcialmente funciones, servicios o infraestructura tecnológica. Se controla mediante KPI, SLA y contratos de soporte, que deben ser monitoreados para garantizar el cumplimiento. Incluye soporte técnico, almacenamiento en la nube, hosting, desarrollo de software, servicios de ciberseguridad, gestión de redes y provisión de equipos.

2.4.5. Gestión de la Continuidad del Negocio

La Gestión de la Continuidad del Negocio asegura la disponibilidad y recuperación de servicios tecnológicos críticos mediante planes y estrategias que permiten mantener o restaurar la operación de los sistemas de TI frente a fallos, ataques cibernéticos, errores humanos o desastres.

2.4.6. Seguridad de la Información

La Seguridad de la Información protege datos y sistemas para garantizar confidencialidad, integridad y disponibilidad, mediante controles físicos y lógicos, políticas de acceso y formación del personal. Incluye la ciberseguridad, orientada a prevenir ciberataques, reducir vulnerabilidades y asegurar la resiliencia y recuperación operativa.

2.4.7. Controles de Aplicación

Los Controles de Aplicación son mecanismos dentro de las aplicaciones informáticas que aseguran la validez, integridad, exactitud y disponibilidad de transacciones y datos, garantizando además el cumplimiento normativo mediante controles de entrada, procesamiento, salida y seguridad.

En función del alcance y del nivel de madurez digital de la entidad, se realizarán pruebas técnicas a los componentes y elementos que los integran, las que permitirán contar con el respaldo del análisis realizado por los auditores, y sustento de las evidencias obtenidas, que serán el insumo para la elaboración de los hallazgos y presentación de los resultados de la auditoría; el alcance y detalle de las pruebas a realizar se encuentran en la sección Pruebas de Auditoría de TI en esta Guía.

3. LIMITACIONES Y EXCLUSIONES

Aunque la Guía busca cubrir de forma amplia la fiscalización de Tecnologías de la Información, existen situaciones en las que la aplicación de las pruebas puede restringirse o requerir adaptaciones especiales; estas limitaciones y exclusiones se describen a continuación:

3.1. LIMITACIONES

Tipo de limitación	Alcance	Tratamiento en la auditoría
a) Causas legales que impiden el análisis del bien o servicio tecnológico adquirido	Proyectos, sistemas o contratos informáticos en litigio o mediación.	Comunicar al responsable de la Unidad de Control para los fines pertinentes e incorporar al informe de auditoría.
b) Limitaciones de acceso a la información	Resistencia del personal auditado para proporcionar información completa y oportuna.	
c) Limitaciones técnicas	Sistemas propietarios o cerrados que no permiten análisis técnico detallado.	
d) Limitaciones organizacionales o de gobernanza	Dependencia de proveedores externos sin contratos claros o con falta de control sobre la calidad del servicio (riesgos de tercerización). Supresión de entidades, procesos, competencias.	

3.2. EXCLUSIONES

Tipo de exclusión	Alcance	Tratamiento en la auditoría
a) Proyectos	Apoyo Técnico especializado	La auditoría se orienta hacia la revisión técnica de los componentes de TI, excluyendo del análisis los que aún no se encuentran implementados, aspectos a constar en el informe de auditoría.
b) Recursos o tiempo insuficientes para pruebas extensivas	Cuando la criticidad es alta y la materialidad del riesgo es representativa.	Se documenta la justificación y se incorpora al informe de auditoría con la finalidad que sea considerado en posteriores acciones de control.

4. MODELO DE MADUREZ DE TI

La madurez de TI (digital) es el estado o nivel de transformación digital actual de una entidad, utilizándolo para describir su grado de adopción de herramientas tecnológicas; también se lo puede definir como el conjunto de niveles estructurados que representan los comportamientos, prácticas y procesos organizacionales que producen de manera confiable y sostenible los resultados requeridos.

Un modelo de madurez requiere como mínimo contar con un marco de referencia que soporte los ítems de evaluación, niveles de capacidad para la escala de evaluación y, las claves de evaluaciones que definan las escalas.

4.1. MARCO DE REFERENCIA

Un Marco de Referencia en el ámbito del desarrollo de un Modelo de Madurez Organizacional basado en el uso de las Tecnologías de la Información (TI) constituye una estructura conceptual y metodológica que guía la evaluación sistemática de las capacidades digitales de una institución; este marco define los criterios clave que deben considerarse como: Dirección de TI, Estado del liderazgo de TI, Gestión estratégica de TI en la entidad, Estado general de informatización de la entidad, Uso de las TI, y Apropiación de tecnología, así también, los indicadores y niveles de desempeño que permiten valorar objetivamente el grado de madurez digital alcanzado y las oportunidades de mejora.

En esencia, el Marco de Referencia actúa como la base sobre la cual se construye el modelo de madurez, asegurando que la evaluación sea coherente, comparable y alineada con las mejores prácticas internacionales; asimismo, facilita el diagnóstico de la situación actual, la definición de metas realistas y la planeación de rutas de transformación digital, permitiendo que la

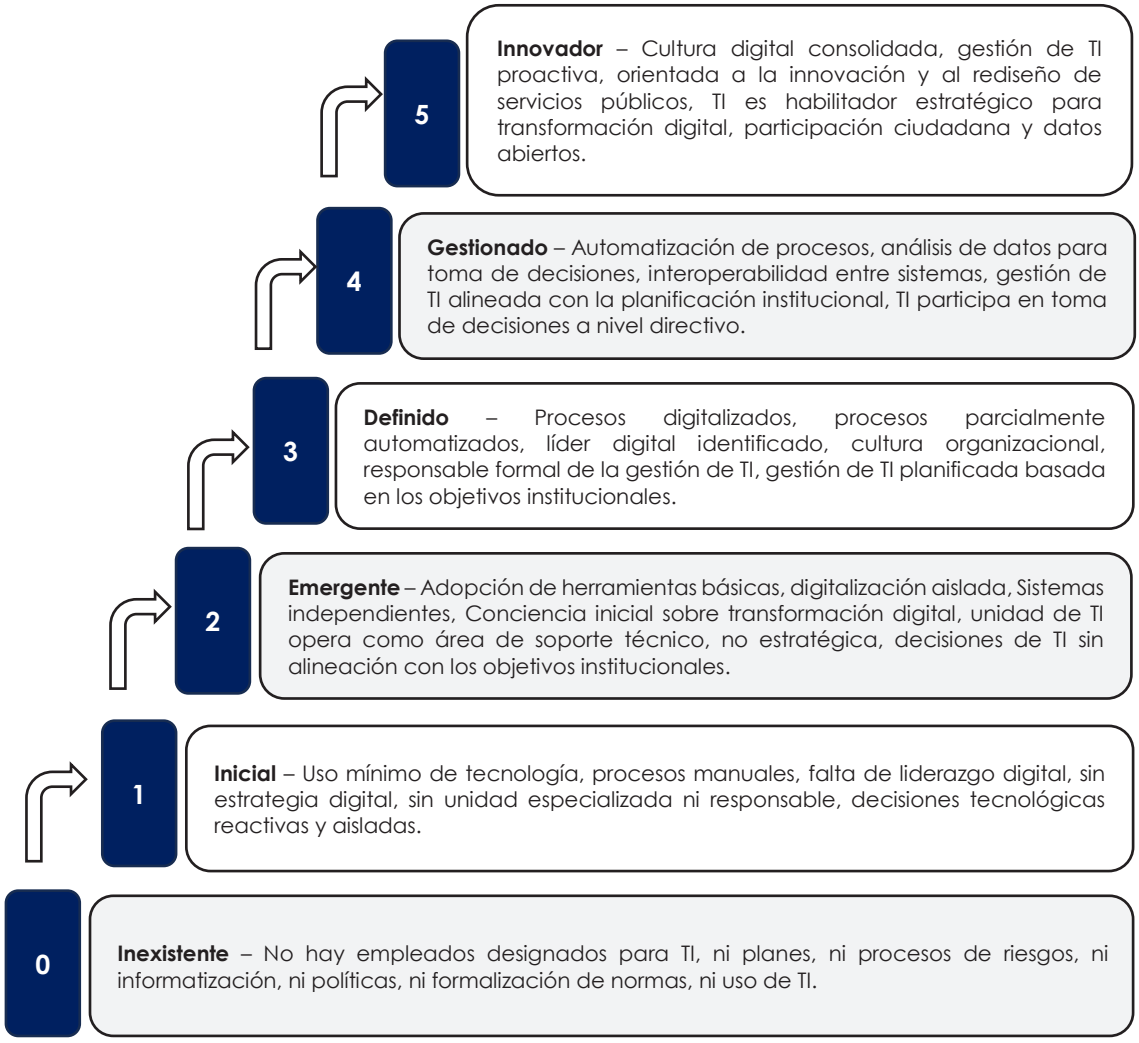
organización adopte estrategias informadas en la gestión y el aprovechamiento de las TI: al integrar lineamientos y estándares reconocidos globalmente, el Marco de Referencia proporciona un lenguaje común y un punto de partida confiable para identificar brechas, priorizar acciones y monitorear avances en el proceso de madurez digital.

4.2. NIVEL DE CAPACIDAD

Un nivel de capacidad puede alcanzarse en distinto grado, lo cual puede expresarse mediante una serie de calificaciones, donde el rango de calificaciones disponible depende del contexto en el que se realiza la evaluación del desempeño.

En ocasiones se requiere un nivel más alto para expresar el desempeño sin la granularidad aplicable a las calificaciones individuales de capacidad de los procesos; igualmente, los niveles de madurez pueden usarse para esos propósitos; el marco define los niveles de madurez como una medida de desempeño, como se muestra a continuación.

Para las evaluaciones organizacionales, los niveles de capacidad están asociados con criterios clave y un cierto nivel de madurez se alcanzará si todos los criterios en las áreas prioritarias alcanzan el nivel de capacidad específico, a continuación, se muestra un ejemplo de Niveles de Madurez Digital para Organizaciones:



Los niveles de capacidad se definen y ajustan de acuerdo con los intereses del evaluador, normalmente obedecen a macro atributos que les permitan la comparabilidad con otras instituciones, de esta manera adquiere sentido la selección de criterios que pueden/o deben estar presentes en todos, y en donde su grado de adopción varíe acorde a su tamaño, importancia y complejidad.

4.3. CLAVES PARA LA EVALUACIÓN

Para la evaluación del nivel de madurez de una institución se establecen criterios organizacionales tal como: Dirección de TI, Estado del liderazgo de TI, Gestión estratégica de TI en la entidad, Estado general de informatización de la entidad, Uso de las TI, Apropiación de tecnología. En cada criterio se proponen atributos a los cuales se les asigna un valor entre paréntesis que se ubican entre 0 y 5, siendo 0 la inexistencia de iniciativa digital, 1 indicativo de menor presencia de los atributos y 5 de mayor presencia.

Se presenta un ejemplo de la evaluación sólo para el criterio "Dirección de TI", considerando que la entidad cumple el atributo: "Se ha designado un responsable formal de la gestión de TI (jefatura o dirección)" la valoración sería la que se encuentra entre paréntesis (3).

	CRITERIOS DE EVALUACIÓN ORGANIZACIONALES	PUNTAJE
1	**Dirección de TI. La entidad ha organizado la dirección, evaluación y toma de decisiones de TI**	
	La gestión de TI es proactiva, orientada a la innovación y al rediseño de servicios públicos. (5)	
	La gestión de TI está alineada estratégicamente con la planificación institucional. (4)	
	Se ha designado un responsable formal de la gestión de TI (jefatura o dirección). (3)	3
	Hay una unidad de TI, pero opera como área de soporte técnico, no estratégica. (2)	
	Existe una unidad especializada, no se ha designado formalmente una persona responsable. (1)	
	No existe una unidad especializada. (0)	

4.4. CALIFICACIÓN DE LA ENTIDAD

En el anexo 1 se presentan todos los criterios; una vez completada la evaluación de todos los criterios organizacionales, se sumarán los puntajes asignados en

cada uno y el total se dividirá por el número de criterios organizacionales evaluados para obtener un promedio; por ejemplo, si las valoraciones de cada uno de los atributos para los criterios del modelo resultaron en lo siguiente:

CRITERIOS	VALOR ATRIBUTO
1. Dirección de TI	2
2. Liderazgo de TI	3
3. Gestión estratégica de TI	2
4. Informatización	3
5. Uso de las TI	2
6. Apropiación de tecnología	3
Suma de los atributos	**15**
Cantidad de Criterios	**6**
PROMEDIO	**2,5**

	CALIFICACIÓN DE LA ENTIDAD	PROMEDIO (1)
	PUNTAJE TOTAL:	**2,5**
	NIVEL DE CAPACIDAD:	**3**
	(1) Redondear arriba cuando decimal >= 5	
NIVEL DE MADUREZ	**DEFINIDO**	

Finalmente, hay resaltar que los riesgos tecnológicos son directamente proporcionales al nivel de madurez, es decir, al grado en que están implementados los elementos de transformación digital en el gobierno y gestión de las entidades.

5. PRUEBAS DE AUDITORÍA DE TI

En la fase de ejecución del proceso de la auditoría, es donde se desarrollan las actividades planificadas en los programas de trabajo y se aplican pruebas según la estrategia y el enfoque definido, a fin de recopilar evidencia suficiente, competente y pertinente que respalde los hallazgos de la auditoría.

Esta guía proporciona una orientación general para realizar las pruebas de auditorías informáticas requeridas por los procedimientos indicados en los programas de trabajo, de acuerdo con lo establecido en el Manual de Auditoría Informática.

Para efectuar los procedimientos establecidos en los programas de auditoría, se deberán realizar pruebas de cumplimiento, pruebas sustantivas o de doble propósito según los resultados de la planificación de la auditoría, a través de las cuales se espera obtener los elementos de juicio pertinentes para detectar, confirmar o delimitar las posibles incidencias o consecuencias que se pueden presentar en la entidad, por la ausencia o incumplimiento de procedimientos básicos y fundamentales para el correcto funcionamiento del componente auditado.

Estas pruebas constituyen una referencia técnica sugerida que podrá ser utilizada por el auditor, siendo un complemento a la documentación formal correspondiente a las plantillas establecidas en el "Anexo 7 - Formato Plan de Pruebas de Auditoría Informática" y el "Anexo 8 - Pruebas para la ejecución de la Auditoría Informática" del Manual de Auditoría Informática. A continuación, se describen los elementos a considerar en las pruebas asociadas a cada uno de los componentes definidos en el apartado 2.6 del Manual, los cuales podrán ser adaptados según el enfoque, alcance y objetivos específicos de la auditoría.

En los anexos 2 al 8 se podrán consultar las matrices sugeridas para las auditorías de cada uno de los componentes y sus respectivos elementos clave, como complemento a lo detallado en el "Anexo 8 - Pruebas para la ejecución de la Auditoría Informática".

ACRÓNIMOS

ABAC: Control de acceso basado en atributos
ACL: Lista de control de acceso
AFD: Agencia Francesa del Desarrollo
AG: Alignment Goal (Meta de Alineamiento de TI)
ANS: Acuerdos de Niveles de Servicio (SLA)
APC: Administración Pública Central
APO: Alinear, Planificar y Organizar (dominio COBIT 2019)
ARCOTEL: Agencia de Regulación y Control de las Telecomunicaciones
BAI: Construir, Adquirir e Implementar (dominio COBIT 2019)
BIA: Business Impact Analysis (Análisis de Impacto al Negocio)
BID: Banco Interamericano de Desarrollo
BSC: Balanced Scorecard (Cuadro de Mando Integral)
BYOD: Trae tu propio dispositivo
CAATs: Computer-Assisted Audit Techniques (Técnicas de Auditoría Asistida por Computadora)
CAF: Corporación Andina de Fomento
CAPTCHA: Prueba de Turing pública completamente automatizada para diferenciar a las computadoras de los humanos
CGE: Contraloría General del Estado
COBIT: Control Objectives for Information and Related Technologies
CPU: Unidad Central de Proceso
DAC: Control de acceso discrecional
DNS: Sistema de Nombres de Dominio
DSS: Entregar, Dar Servicio y Soporte (dominio COBIT 2019)
EDM: Evaluar, Dirigir y Monitorizar (dominio COBIT 2019)
EFS: Entidad Fiscalizadora Superior
EG: Enterprise Goal (Meta Institucional)
EGSI: Esquema Gubernamental de Seguridad de la Información
E-procurement: Aprovisionamiento electrónico

ERP:	Enterprise Resource Planning (Planificación de Recursos Empresariales)
GAD:	Gobierno Autónomo Descentralizado
GATI:	Guía Técnica para la Realización de Auditorías Informáticas
GPS:	Sistema de Posicionamiento Global
IaaS:	Infraestructura como Servicio (Infrastructure as a Service)
IAM:	Identity and Access Management (Gestión de Identidades y Accesos)
ID:	Identificación
IDE:	Entorno de Desarrollo Integrado
IDS:	Sistema de Detección de Intrusos
IESS:	Instituto Ecuatoriano de Seguridad Social
IoT:	Internet de las Cosas
IP:	Protocolo de Internet
IPS:	Sistema de Prevención de Intrusiones
ISSAI:	International Standards of Supreme Audit Institutions
ISSFA:	Instituto de Seguridad Social de las Fuerzas Armadas
ISSPOL:	Instituto de Seguridad Social de la Policía Nacional
ITSM:	IT Service Management (Gestión de Servicios de TI)
KPI:	Key Performance Indicator (Indicador Clave de Desempeño)
KRI:	Key Risk Indicator (Indicador Clave de Riesgo)
LAN:	Red de área local (Inglés Local Área Network)
LOCGE:	Ley Orgánica de la Contraloría General del Estado
LOPDP:	Ley Orgánica de Protección de Datos Personales
MAC:	Control de acceso obligatorio
MEA:	Monitorizar, Evaluar y Valorar (dominio COBIT 2019)
MGGTI:	Marco de Gobierno y Gestión de Tecnologías de la Información
MINTEL:	Ministerio de Telecomunicaciones y de la Sociedad de la Información
MSP:	Ministerio de Salud Pública
NCI:	Normas de Control Interno
NTP:	Protocolo de Tiempo de Red
PaaS:	Plataforma como Servicio (Platform as a Service)

PAC:	Plan Anual de Control
PETI:	Plan Estratégico de Tecnologías de la Información
PIA:	Evaluación de Impacto de Privacidad
PII:	Información Personal Identificable
PIN:	Número de Identificación Personal
PKI:	Infraestructura de Clave Pública
POA:	Plan Operativo Anual
PTP:	Protocolo de Tiempo de Precisión
RBAC:	Control de acceso basado en roles
RPO:	Punto de Recuperación Objetivo
RRHH:	Recursos Humanos
RTO:	Tiempo Objetivo de Recuperación
SaaS:	Software como Servicio (Software as a Service)
SAST:	Pruebas de Seguridad de Aplicaciones
SD:	Seguro Digital
SDN:	Redes Definidas por Software
SD-WAN:	Red de Área Amplia Definida por Software
SERCOP:	Servicio Nacional de Contratación Pública
SGSI:	Sistema de Gestión de Seguridad de la Información
SIEM:	Gestión de Eventos e Información de Seguridad
SIGEF:	Sistema Integrado de Gestión Financiera (eSIGEF)
SIG:	Sistema de Información Geográfica (GIS en inglés)
SMS:	Servicio de Mensajes Cortos
SOC:	Security Operations Center (Centro de Operaciones de Seguridad)
SoD:	Segregation of Duties (Separación de Funciones)
SQL:	Lenguaje de Consulta Estructurado
SSO:	Inicio de Sesión Único
SWID:	Identificación del Software
TI:	Tecnologías de la Información
TIC:	Tecnologías de la Información y Comunicación
UEBA:	Análisis de Comportamiento de Usuarios y Entidades
UPS:	Fuente de Alimentación Ininterrumpida
URL:	Localizador Uniforme de Recursos

USB: Bus Serie Universal

VM: Máquina Virtual

VPN: Red Privada Virtual

WAN: Red de área amplia (Inglés Wide Área Network)

WIFI: Fidelidad Inalámbrica

GLOSARIO DE TÉRMINOS

Aceptar el Riesgo: Es uno de los métodos más comunes de manejar el riesgo, es la decisión de aceptar las consecuencias de la ocurrencia del evento.

Actividades de Control: Según COSO, hace referencia a los controles que realmente existen para minimizar los riesgos que enfrenta la empresa.

Activos: Son los recursos del Ente o relacionados con éste, necesarios para que la organización funcione correctamente y alcance los objetivos propuestos por su dirección.

Administración del Riesgo: Es un proceso que asegura la sensibilidad para detectar el riesgo, la flexibilidad para responder al riesgo, y la capacidad de recursos para mitigar los riesgos.

AICPA: American Institute of Certified Public Accountants – Instituto Americano de Contadores Públicos Certificados.

Ambiente de Control: Según COSO, hace referencia a la cultura corporativa de control que debe existir en una organización.

Amenaza: Es un factor del medio ambiente externo que puede ocasionar una falla en el desempeño futuro de las organizaciones. Se definen como los eventos que pueden desencadenar un incidente en la organización, produciendo daños materiales o pérdidas inmateriales en sus activos. Las Amenazas se pueden materializar y transformarse en agresiones.

Análisis de Campo de Fuerza: Es una técnica utilizada para lograr una perspectiva completa de las fuerzas en pro y en contra de un plan, de manera que una decisión puede ser tomada teniendo en cuenta todos los intereses.

Ayuda a reducir el impacto de las fuerzas en oposición, y fortalecer las fuerzas soporte.

Análisis DOFA: Este tipo de análisis examina la interacción entre las características particulares de la organización y el medio ambiente en el cual se desenvuelve.

Aplicaciones: Recurso de TI, definido como sistemas de aplicación; la suma de procedimientos manuales y programados.

Árboles de Decisión: Herramientas de gran relevancia para la toma de decisiones basada en aspectos financieros o en situaciones que impliquen números, donde se debe tener en cuenta una gran cantidad de información. Básicamente su estructura permite contemplar y evaluar alternativas y las implicaciones de tomar esas decisiones, permitiendo visualizar los riesgos que pueden derivarse de algunas alternativas.

Asumir el Riesgo: ver "Aceptar el riesgo".

Auditoría basada en los Riesgos (ABR): metodología que se está empezando a implementar como parte del cambio al nuevo paradigma. Esta metodología tiene en cuenta los objetivos organizacionales para la evaluación de los riesgos y dar en su informe las recomendaciones pertinentes sobre la mejor forma de manejar dichos riesgos.

Auditoría de Cumplimiento: consiste en la comprobación o examen de las operaciones financieras, administrativas, económicas y de otra índole de una entidad para establecer que se han realizado conforme a las normas legales, estatutarias y de procedimientos que le son aplicables.

Auditoría de Gestión: Este tipo de auditoría se encarga de evaluar el grado de eficacia y eficiencia con que se manejan los recursos de la entidad, y el grado de eficacia y eficiencia con que se logran los objetivos organizacionales.

Auditoría de Protección de Datos: Examen practicado para verificar que los datos electrónicos que maneja la organización poseen las medidas de seguridad apropiadas para evitar su conocimiento masivo y su potencial modificación ya sea parcial o total por parte de terceros.

Auditoría Financiera: examen de las operaciones financieras llevadas a cabo por una entidad con el fin de evaluarlas y verificarlas con posterioridad a su ejecución para determinar la razonabilidad de las cifras contenidas en los estados financieros.

Auditoría Integral: es una auditoría que, como su nombre lo indica, integra en una sola labor la práctica de las auditorías financiera, de cumplimiento, de gestión y de control interno.

Auditoría Interna: La Auditoría Interna es una actividad de aseguramiento y de consultoría independiente y objetiva, diseñada para adicionar valor y mejorar las operaciones de una organización. La Auditoría Interna ayuda a la organización a lograr sus objetivos brindando un enfoque sistemático y disciplinado para evaluar y mejorar la efectividad de los procesos de administración del riesgo, de control y de gobierno corporativo.

Balanced Scorecard: Esta metodología es un enfoque gerencial que, según sus creadores Robert Kaplan y David Norton, traduce las estrategias en mediciones que comuniquen la visión corporativa a toda la organización.

Benchmarking: el proceso de medir las operaciones de una organización contra operaciones similares con el propósito de mejorar los procesos del negocio. Su propósito es mejorar los productos y procesos para satisfacer mejor las necesidades de los clientes. Es decir, mirar lo que han hecho con éxito otras empresas de la misma industria en cuanto administrar los riesgos, y realizar las mismas acciones; en caso de que aquellas empresas no hayan tenido buenos

resultados, tener en cuenta esas situaciones para mejorarlas o para no realizarlas.

Cambio: es el proceso de adaptación de un sistema u organización con su medio ambiente.

Capacidad: es un grupo de criterios que proveen un sentido de la competencia de la organización.

CICA: Canadian Institute of Chartered Accountants – Instituto Canadiense de Contadores Certificados.

Ciclo del Cambio: modelo desarrollado por David MacNamee para entender las fases de crecimiento de un sistema u organización. Este ciclo no es lineal ni circular, sino que presenta las características de una espiral. El ciclo del cambio presenta tres fases: formación, normalización y cumplimiento; separadas por límites críticos, llamados breakpoints.

COBIT: Informe emitido por la Information Systems Audit and Control Foundation, órganos dependientes de ISACA que muestra procedimientos de auditoría que se pueden efectuar sobre sistemas de información.

COCO: Acrónimo de **C**riteria **o**f **Co**ntrol, una iniciativa del Canadian Institute of Chartered Accountants (CICA) para proveer una estructura de control, para el fortalecimiento del control y del gobierno corporativo en una organización.

Código CADBURY (Cadbury Code): Metodología desarrollada por el Comité de Informes Financieros del Institute of Chartered Accountants of England and Wales (ICAEW) como un informe de riesgo.

Compartir el Riesgo: es un caso especial de la transferencia del riesgo, es también una forma de retener el riesgo. Cuando los riesgos son compartidos, la posibilidad de pérdida es transferida de un individuo al grupo; sin embargo,

compartir el riesgo es también una forma de retenerlo en la cual el riesgo "transferido" al grupo es retenido junto con los riesgos de los demás miembros del grupo.

Compromiso: Para CoCo, es un grupo de criterios que proveen un sentido de la identidad y valores de la organización.

Confiabilidad de la Información: Criterio de información de COBIT que hace referencia a la provisión de información apropiada para la administración con el fin de operar la entidad y para ejercer sus responsabilidades de reportes financieros y de cumplimiento.

Confidencialidad: Criterio de información de COBIT que hace referencia a la protección de información sensible contra divulgación no autorizada.

Contraloría: Organismo de control que vigila la gestión fiscal de la administración y de los particulares o entidades que manejen fondos o bienes de la Nación.

Control Interno: sistema integrado por el esquema de organización y el conjunto de los planes, métodos, principios, normas, procedimientos y mecanismos de verificación y evaluación adoptados por una entidad, con el fin de procurar que todas las actividades, operaciones y actuaciones, así como la administración de la información y los recursos, se realicen de acuerdo con las normas constitucionales y legales vigentes dentro de las políticas trazadas por la dirección y en atención a las normas u objetivos previstos.

Control: Según CoCo, son todos los elementos de una organización, incluyendo sus recursos, sistemas, procesos, cultura, estructura y tareas –, que tomados en conjunto respaldan a la gente en el logro de los objetivos de la organización.

Controlar el Riesgo: el riesgo se controla a través de la prevención por medio de la implementación de controles y su monitoreo constante. Esta es una técnica ideal para el manejo de los riesgos, y es la más utilizada

COSO: Metodología de control emitida por el **C**ommittee **of S**ponsoring **O**rganizations of the Treadway Commission.

COSTO: Impacto sobre el precio que se pagaría si se presenta un riesgo determinado.

CSA: Acrónimo de **C**ontrol **S**elf-**A**ssessment (Autoevaluación de Control) y es definido por McNamee como "la involucración de la gerencia y el personal en la evaluación de los controles internos dentro de su grupo de trabajo".

Cumplimiento: Criterio de información de COBIT que hace referencia al cumplimiento de aquellas leyes, regulaciones y acuerdos contractuales a los que el proceso de negocios está sujeto, por ejemplo, criterios de negocio impuestos externamente.

Curva Estratégica Riesgo/Oportunidad: modelo desarrollado por David McNamee para mostrar la relación entre los conceptos de riesgo y oportunidad. Muestra además los efectos que tiene el tiempo (corto, mediano y largo plazo) sobre estos dos conceptos.

D.A.R.E.: "Valoración Dinámica de Riesgos y Factores de Riesgo" – proviene su nombre del nombre en inglés "**D**ynamic **A**ssessment of **R**isk and **E**nablers"–. Metodología informática aplicable en Auditoría Interna.

Datos: Recurso de TI en COBIT, definido como los elementos de datos en su más amplio sentido, (por ejemplo, externos e internos), estructurados y no estructurados, gráficos, sonido, etc.

Debilidad: algo de lo que carece una compañía o ejecuta deficientemente comparado con los rivales o una condición que la coloca en una desventaja competitiva.

Diagrama Causa – Efecto: Este es un diagrama con forma de espina de pescado que muestra la relación entre los efectos que genera un proceso o actividad, y las posibles causas que lo originan.

Diagrama de Dispersión: Este gráfico representa la relación que existe entre dos variables, ubicando en el eje x la que se considera como posible causa, y en el eje *y*, la variable que se considera como efecto. Al marcar las parejas de puntos se forma una "nube" que permite llevar a cabo el análisis de dependencia entre las variables en estudio.

Diagrama de Flujo: Representación gráfica de las actividades o pasos a seguir para llevar a cabo un proceso. Se ha de tener en cuenta la secuencialidad, la relación entre dichas actividades, y los productos que se generan en cada uno de estos pasos.

Diagrama de Pareto: Diagrama basado en el "principio de Pareto", según el cual en la aparición u obtención de un efecto hay muy pocas causas realmente importantes que son responsables del 80% del total del efecto, y muchas causas secundarias que son responsables solamente del 20% restante. Es decir, hay muy pocos factores vitales y muchos triviales.

Diagrama GRID: Este diagrama es una herramienta utilizada para llevar a cabo de manera apropiada la priorización de procesos o actividades para de esta manera poder concentrar el trabajo de auditoría en aquellos que presenten un mayor nivel de riesgo.

Disponibilidad: Criterio de información de COBIT que hace referencia a la disponibilidad de la información cuando ésta es requerida por el proceso de

negocio ahora y en el futuro. También se refiere a la salvaguarda de los recursos necesarios y capacidades asociadas.

Diversificar el Riesgo: ver "Compartir el riesgo".

Ecología: Factor de evaluación de los procesos en que se mide el adecuado manejo de los recursos naturales.

Economía: Factor de evaluación de los procesos en que se mide el si se produce un mayor beneficio con un mínimo costo.

Efectividad: Criterio de información de COBIT que hace referencia a que la información relevante sea pertinente para el proceso del negocio, así como a que su entrega sea oportuna, correcta, consistente y de manera utilizable.

Eficacia: Factor de evaluación de los procesos en que se mide el logro apropiado de los objetivos.

Eficiencia: (1) Factor de evaluación de los procesos en que se mide el manejo apropiado de los recursos. (2) Criterio de información de COBIT que hace referencia a la provisión de información a través de la utilización óptima (más productiva y económica) de recursos.

Equidad: Factor de evaluación de los procesos en que se mide la imparcialidad en el trato y la justicia natural.

Ética: Factor de evaluación de los procesos en que se mide la solidez de los principios morales de la organización.

Evaluación de Riesgos: Según COSO, es el examen de factores internos y externos que impiden el logro de los objetivos organizacionales.

Evaluación Hipotética de Riesgos: Evaluación de riesgos que se efectúa en la fase de planeación, que se basa en el análisis del diagrama de flujo y los aportes de los responsables del (los) proceso(s) estudiado(s).

Evaluación Práctica de Riesgos: Evaluación de riesgos que se efectúa en el trabajo de campo, en que confronta los riesgos observados con los factores de riesgos para determinar las causas que originan la ocurrencia de los riesgos observados.

Evaluación Preliminar de Riesgos: Evaluación de riesgos que se efectúa en la fase de evaluación de los controles, que se basa en el análisis realizado en la evaluación hipotética de riesgos y el estudio de la fortaleza del sistema de Control Interno.

Evitar el Riesgo: el riesgo es evitado cuando la organización rechaza aceptarlo, es decir, no se permite ningún tipo de exposición. Esto se logra simplemente con no comprometerse con la acción que origine el riesgo.

Fase de Cumplimiento: fase del ciclo del cambio donde existe la conciencia que al tiempo que un sistema u organización crece a través del mejoramiento, al interior del medio ambiente que los rodea se producen cambios de muchas maneras. El sistema u organización debe reaccionar ante estos cambios incorporando lo nuevo y lo diferente.

Fase de Formación: fase del ciclo del cambio donde la organización o el sistema trata de establecer una conexión segura con su medio ambiente. Es una época de gran experimentación, de probar nuevas ideas, de responder rápida y furiosamente al mercado.

Fase de Normalización: fase del ciclo del cambio donde se mantienen vínculos regulares y repetibles con el medio ambiente y se refuerza la conexión que dio resultado. El sistema u organización se concentra en repetir lo que fue exitoso; se decide lo que se hará y lo que no se hará.

Fase de Renovación: fase del ciclo del cambio que representa una nueva fase de formación. Se hacen mejoras a la calidad más que a la cantidad, hay más innovación, el sistema u organización empiezan a reinventarse. Empieza un nuevo ciclo de crecimiento.

Frecuencia: Repetición frecuente de un riesgo sobre una actividad específica.

Gobierno: Según CoCo, hace referencia a los procesos y estructuras utilizados para dirigir y gerenciar la organización. Hace referencia al rol de la Alta Gerencia y de la Junta Directiva.

Hacker: Pirata cibernético encargado de penetrar en las redes computacionales de las empresas para extraer información ya sea de carácter general o específica.

Hoja de Verificación: Herramienta útil para el registro y organización de la información requerida al momento de realizar un análisis sobre un departamento, sistema, proceso o actividad.

IIA: Institute of Internal Auditors – Instituto de Auditores Internos.

Impacto: Repercusión directa de un riesgo en un proceso y/o sistema determinado.

Impacto: Según Magerit se define como un daño producido a la organización por un posible incidente y es el resultado de la Agresión sobre el Activo, o visto de manera más dinámica, la diferencia en las estimaciones de los estados (de seguridad) obtenidas antes y después del evento.

Incertidumbre: según Emmet Vaughan, es una reacción psicológica a la ausencia de conocimiento acerca del futuro. Con base en la teoría de la probabilidad, se puede medir en un intervalo entre 0 y 1.

Información y Comunicación: Según COSO, es el proceso de retroalimentación que debe existir dentro de la empresa y entre ésta y su medio ambiente.

Instalaciones: Recurso de TI en COBIT, definido como los recursos para alojar y dar soporte a los sistemas de información.

Integridad: Criterio de información de COBIT que hace referencia a la precisión y suficiencia de la información, así como a su validez de acuerdo con los valores y expectativas del negocio.

ISACA: Information Systems Audit and Control Asociation.

IT: Information Technology – Tecnología de Información.

Lluvia de Ideas: Técnica en la cual un grupo o grupos del personal de la organización colaboran con la generación de ideas acerca de un tema específico de acuerdo con la índole de cada grupo. Durante la sesión no se permite la crítica – en su sentido negativo – de las ideas expuestas.

MAGERIT: Metodología de **A**nálisis y **Ge**stión de **R**iesgos de los sistemas de **I**nformación de las Adminis**t**raciones Públicas elaborada por el Consejo Superior de Informática, cuya utilización promueve, como respuesta a la dependencia creciente de éstas (y en general de toda la sociedad) respecto a las Tecnologías de la Información.

Matriz Crecimiento – Participación: Técnica utilizada para analizar las operaciones de una empresa diversificada y verla como un portafolio de negocios. Aporta un marco de referencia para categorizar los diferentes negocios de una organización y determinar sus implicaciones en cuanto a asignación de recursos.

Matriz de Prioridades: Matriz de prioridades complementaria al análisis DOFA, pues realiza un análisis de las debilidades y/o amenazas y de las fortalezas y/u oportunidades a los que se enfrenta una organización.

Monitoreo y Aprendizaje: Para CoCo, es un grupo de criterios que proveen un sentido de la evolución de la organización.

Monitoreo: Según COSO, se refiere al seguimiento permanente que se debe hacer, por parte de la administración, para evaluar la efectividad del sistema de control interno

Oportunidad: para McNamee, la oportunidad es "el potencial de resultados positivos – más de lo esperado –, y el riesgo es "el potencial de resultados negativos – menos de lo esperado –, derivados de los cambios ocurridos en el ambiente donde se desenvuelven las organizaciones.

Paradigma: principios o dogmas que se catalogan como verdad en una rama del conocimiento y que prevalecen por cierto tiempo hasta que, debido a cambios en el medio ambiente, surgen nuevos principios y métodos, con lo cual se genera un cambio de paradigma.

Paradigmas en Auditoría: la auditoría ha pasado por dos paradigmas y está entrando a un tercero. Estos paradigmas son: auditoría basada en la re-ejecución o verificación total de las operaciones; auditoría basada en los controles internos, y; auditoría basada en los riesgos del negocio.

Problema: Es como el efecto adverso que indefectiblemente surge ante la ocurrencia de un riesgo y que siempre se manifiesta en términos de trastornos o daños.

Proceso de la Administración del Riesgo: comprende las siguientes fases: determinación de objetivos, identificación de riesgos, evaluación de riesgos,

consideración de alternativas y selección de la(s) técnica(s) de manejo de(los) riesgo(s), implementación de la decisión tomada, y evaluación y revisión del proceso.

Propósito: Para CoCo, es un grupo de criterios que proveen un sentido de la dirección de la organización.

Reducir el Riesgo: ver "controlar el riesgo".

Relación con Clientes Externos: Relación directa de la ocurrencia de un riesgo sobre terceros.

Relación con Clientes Internos: Relación directa de la ocurrencia de un riesgo sobre los empleados de la organización.

Retener el Riesgo: ver "Aceptar el riesgo".

Revisoría Fiscal: es un órgano de fiscalización que, en interés de la comunidad, bajo la dirección y responsabilidad del revisor fiscal y con sujeción a las normas de auditoría de general aceptación, le corresponde dictaminar los estados financieros y revisar y evaluar sistemáticamente los componentes y elementos que integran el control interno, en forma oportuna e independiente en los términos que le señale la ley, los estatutos y los pronunciamientos profesionales.

Riesgo: es una medida de incertidumbre que refleja hechos presentes o futuros que pueden ocasionar una ruptura en el flujo de información o incumplimiento en el logro de los objetivos organizacionales.

Riesgo Absoluto: El máximo riesgo sin los efectos mitigantes de controles internos.

Riesgo Administrado: Los riesgos y consecuencias después de la aplicación del control interno.

Riesgo de Ambiente de Operación: Son amenazas que surgen como consecuencia de procesos inefectivos o ineficientes para la adquisición, transformación y mercadeo de bienes y servicios, así como detrimento de activos físicos, financieros, de información, o intelectuales; pérdidas de mercado u oportunidades de mercado y; perjuicio en la reputación.

Riesgo de Ambiente Estratégico: Son amenazas de los factores externos al negocio, incluyendo cambios en los gustos y preferencias de los clientes, creación de productos sustitutos o cambios en el ambiente competitivo, escenarios políticos, ambiente legal y normativo, y disponibilidad de capital.

Riesgo de Capacidad Directiva: Factor interno que hace referencia a la competitividad del recurso humano, incluyendo variables como: Nivel académico, experiencia, estabilidad, rotación, capacitación y programas de desarrollo, entre otras.

Riesgo de Competencia: Factor interno y/o externo que se deriva con el mercado, y su área comercial en la venta de productos o prestación de servicios, y está encaminado a determinar la oportunidad y la capacidad de competencia que tiene la organización en el medio. Incluye variables como: Portafolio de productos, calidad del producto, canales de distribución, investigación y desarrollo, servicio al cliente, entre otras.

Riesgo de Conocimiento: Factor interno que se deriva de la cultura estratégica; reconocimiento de la organización en cada una de sus facetas; visión, misión, objetivos globales, estrategias, cultura institucional, planes de acción, políticas, normas, procedimientos, filosofía de la administración, estilo de operación, proceso administrativo; y, conocimiento del Control Interno.

Riesgo de Control: La tendencia del sistema de control interno de perder eficacia con el paso del tiempo y exponer, o no impedir la exposición de los activos que salvaguarda.

Riesgo de Detección: La probabilidad que se obtendrá una conclusión de auditoría errada a partir de los resultados de un examen.

Riesgo de Empresa: el riesgo proveniente de las estrategias y objetivos específicos de la unidad de negocio.

Riesgo de Entorno: ver "Riesgos externos".

Riesgo de Funciones: Es el riesgo sobre un proceso industrial.

Riesgo de Información: Son amenazas de uso de información de poca calidad para la toma de decisiones operacional, financiera o estratégica dentro del negocio y suministrar información distorsionada a terceras personas.

Riesgo de Cultura de Control: el riesgo proveniente de los elementos de las organizaciones (recursos, sistemas, procesos, cultura, estructura y tareas) que tomadas en conjunto apoyan a la gente en el logro de los objetivos de la compañía.

Riesgo de Liquidez: Se refiere a la disponibilidad de recursos cuando son necesarios, al flujo continuo y consistente de estos recursos y la confianza de que continúen circulando.

Riesgo de Planeación: Es el riesgo que el proceso de planeación sea defectuoso. En términos de evaluación de riesgos, es el riesgo de que el proceso de evaluación sea inadecuado o incorrectamente implementado.

Riesgo de Políticas: Es el riesgo que el diseño de las políticas de la organización sea deficiente.

Riesgo de Portafolio: Es el riesgo de que una combinación de proyectos, activos, unidades o lo que exista en cartera no alcance para lograr los objetivos totales de la cartera debido a una mala balanza de riesgos dentro de la misma.

Riesgo de Proceso: el riesgo proveniente de los procesos y productos clave utilizados para lograr las estrategias y los objetivos específicos de la unidad de negocio. Es el riesgo sobre un proceso comercial.

Riesgo de Producción: Es simplemente el riesgo asociado con las capacidades de fabricación y producción, el grado de adaptación al cambio de estos procesos y su grado de disponibilidad o no disponibilidad.

Riesgo de Recurso Humano: Son los que pueden afectar la productividad y efectividad organizacional.

Riesgo de Reputación: Es el riesgo de una pérdida de confianza en la administración de la organización.

Riesgo del Negocio: (1) según el AICPA, es definido como la amenaza que un evento o acción afecte de manera adversa la habilidad de la organización para lograr sus objetivos corporativos y ejecutar exitosamente sus estrategias. (2) Ver Riesgo de Empresa.

Riesgo Dinámico: Los riesgos dinámicos son los que resultan de los cambios en la economía; surgen de dos tipos de factores: Factores en el medio externo, los cuales son incontrolables y los otros factores son las decisiones gerenciales dentro de la empresa.

Riesgo Económico: Factor externo que se relaciona con el comportamiento de la economía, tanto al nivel nacional como internacional; que tiene como característica particular que el efecto de sus variables es explosivo y pueden

incluirse –entre otras– las siguientes: Inflación, PIB, ingreso per cápita, devaluación, comportamiento de la economía internacional.

Riesgo Específico: Es el tipo de riesgo que recae sobre una actividad específica, debido a que el nivel de riesgo varía de actividad en actividad.

Riesgo Especulativo: El riesgo especulativo describe una situación que sostiene la posibilidad tanto de pérdida como de ganancia.

Riesgo Estático: Los riesgos estáticos involucran aquellas pérdidas que resultarían aun si no ocurren cambios en la economía.

Riesgo Estratégico: el riesgo proveniente de las estrategias y objetivos globales de la organización.

Riesgo Externo: resultan de circunstancias ajenas a la empresa que pueden ser difíciles o imposibles de controlar. Estos riesgos serían causados, en su mayoría, por fuerzas sociales, políticas o económicas.

Riesgo Financiero: (Factor Interno que se relaciona directamente con el Capital de Trabajo, las fortalezas o debilidades financieras de la organización, en el manejo de sus finanzas, e incluye variables como: Liquidez, endeudamiento, margen de rentabilidad, rotación de activos corrientes y elasticidad en la demanda, entre otras. Se pueden considerar como parte de los riesgos internos y pueden ser resumidos como el riesgo que los flujos de caja no sean administrados efectivamente para: maximizar la disponibilidad del efectivo; para reducir incertidumbre en cuanto a la variación en la moneda, tasas de interés y créditos; y para mover fondos de efectivo de manera rápida y sin pérdida de valor a donde más se necesiten. Estos riesgos pueden tener un efecto directo en los activos y pasivos monetarios. (3) riesgo financiero involucra la relación entre un individuo, o una organización, y un activo o un ingreso que se puede perder o dañar.

Riesgo Fiscal: El riesgo de que las deficiencias en el control de gastos o ingresos afecten de manera adversa el logro de los objetivos.

Riesgo Inherente: Es el que tiene que ver con la naturaleza propia de cada actividad.

Riesgo No Financiero: este término describe aquellos riesgos que no se relacionan directamente con los activos y pasivos monetarios. Sin embargo, estos riesgos tienen implicaciones financieras para los flujos de caja y la obtención de utilidades, aunque incluyen riesgos de salud y seguridad, decisiones políticas y cambios que afectan al negocio.

Riesgo Operativo: riesgo asociado con el ¿Qué tan bien operan los sistemas en cuanto a especificaciones de diseño o seguridad?

Riesgo Residual: Es el riesgo que queda cuando han sido aplicadas las técnicas de administración o manejo de riesgos.

Riesgo Tecnológico: Factor Interno y/o externo que incluye aspectos relacionados con el uso de tecnología tangible o intangible, infraestructura tecnológica, normalización de procesos, y la capacidad de reacción que tiene la organización en el uso de éstas.

Sanción Legal: Pago de una multa ante las autoridades tributarias, civiles, laborales, entre otras.

Tecnología: Recurso de TI en COBIT, definido que cubre hardware, software, sistemas operativos, sistemas de administración de bases de datos, redes, multimedia, etc.

Transferir el Riesgo: El riesgo puede ser transferido de una organización a otra que tenga más capacidad de tratarlo.

Valuación de Riesgos: Según COSO, es un componente del control que da una perspectiva acerca de la eficiencia de los controles.

Vulnerabilidad: Se define como la ocurrencia real de materialización de una Amenaza sobre un Activo.

ANEXOS

ANEXO 1. TABLA DE EVALUACIÓN DE MODELO DE MADUREZ DIGITAL

ANEXO 2. GOBERNANZA Y GESTIÓN DE TI

ANEXO 3. DESARROLLO Y ADQUISICIÓN DE TI

ANEXO 4. OPERACIONES DE TI

ANEXO 5. EXTERNALIZACIÓN

ANEXO 6. GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO

ANEXO 7. SEGURIDAD DE LA INFORMACIÓN

ANEXO 8. CONTROLES DE APLICACIÓN

ANEXO 1. TABLA DE EVALUACIÓN DE MODELO DE MADUREZ DIGITAL

	CRITERIOS DE EVALUACIÓN ORGANIZACIONALES	PUNTAJE
1	**Dirección de TI. La entidad ha organizado la dirección, evaluación y toma de decisiones de TI**	
	La gestión de TI es proactiva, orientada a la innovación y al rediseño de servicios públicos. (5)	
	La gestión de TI está alineada estratégicamente con la planificación institucional. (4)	
	Se ha designado un responsable formal de la gestión de TI (jefatura o dirección). (3)	
	Hay una unidad de TI, pero opera como área de soporte técnico, no estratégica. (2)	
	Existe una unidad especializada, no se ha designado formalmente una persona responsable. (1)	
	No existe una unidad especializada. (0)	
2	**Estado del liderazgo de TI**	
	Liderazgo visionario e innovador, el liderazgo de TI impulsa la transformación digital (5)	
	Liderazgo activo y orientado a resultados, TI impulsa proyectos estratégicos (4)	
	Liderazgo con rol organizacional claro, existe planificación estratégica de TI (3)	
	Liderazgo funcional, limitado, algunas decisiones de TI tienen apoyo gerencial (2)	
	Liderazgo reactivo o inexistente, no hay visión clara de TI (1)	
	No existe liderazgo formal ni visión de TI. La gestión tecnológica es improvisada o dejada al azar (0)	
3	**Gestión estratégica de TI en la entidad. La entidad ha establecido alineación de TI**	
	TI es un habilitador estratégico para transformación digital, participación ciudadana y datos abiertos (5)	
	Participa en la toma de decisiones a nivel directivo. (4)	
	La gestión de TI se planifica con base en los objetivos institucionales (3)	
	Las decisiones las toma la unidad de TI sin alineación con los objetivos institucionales (2)	
	Las decisiones tecnológicas se toman de forma reactiva y aislada (1)	
	Sin planes establecidos (0)	
4	**Estado general de informatización de la entidad. La entidad ha informatizado:**	
	Proceso automatizados y uso de inteligencia artificial, bigdata, IoT, etc. (5)	
	Procesos optimizados con tecnología. (4)	
	Procesos parcialmente automatizados (3)	

	Digitalización aislada (2)	
	Procesos manuales (1)	
	Ningún proceso de la institución (0)	
5	**Uso de las TI**	
	Cultura digital consolidada (5)	
	Automatización de procesos (4)	
	Procesos digitalizados (3)	
	Adopción de herramientas básicas (correo, ofimática) (2)	
	Uso mínimo de tecnología (1)	
	No existe adopción de TI (0)	
6	**Apropiación de tecnología**	
	Cultura ágil y centrada en el usuario (5)	
	Análisis de datos para toma de decisiones (4)	
	Cultura organizacional empieza a cambiar (3)	
	Conciencia inicial sobre transformación digital (2)	
	No hay estrategia digital clara (1)	
	Sin estrategia digital (0)	
	CALIFICACIÓN DE LA ENTIDAD	**PROMEDIO** (1)
	PUNTAJE TOTAL:	**XX**
	NIVEL DE CAPACIDAD (1) Redondear al arriba cuando decimal >= 5	

ANEXO 2. - GOBERNANZA Y GESTIÓN DE TI

MATRIZ SUGERIDA PARA LA AUDITORÍA

1.1 Estrategia y Planificación de TI	
Objetivo de auditoría: Evaluar si la Dirección de la organización conduce, evalúa y monitorea efectivamente el uso de TI para el cumplimiento de la misión institucional. Confirmar si existe una estrategia de TI, incluido el plan de TI y los procesos para el desarrollo de la estrategia, aprobación, implementación y mantenimiento, que se adapte a las estrategias y objetivos de la organización. Verificar que, mientras se da cumplimento a los objetivos de TI, los riesgos y recursos son gestionados con eficacia.	
Tema 1 de auditoría: Definir los requerimientos de TI y se establecen estrategias ¿De qué manera la organización identifica y aprueba los requerimientos del institucionales de TI? ¿Cuenta la organización con una estrategia de TI que sirva para guiar sus funciones de TI?	
Criterios: • La organización cuenta con una planificación con la identificación priorizada de los proyectos y las necesidades de TI, y el Comité de Gobernanza de TI tiene suficiente información para tomar sus decisiones y aprobar los requerimientos.	
Información Requerida	**Método(s) de Análisis**
Proceso de gestión de requerimientos institucionales Informe del área de planificación relevando las motivaciones sobre requerimientos de TI. Actas del Comité de Gobernanza aprobando requerimientos Lista de requerimientos aprobados y rechazados Plan Estratégico de TI, o documento equivalente Actas de reunión de TI y reuniones del Comité de Gobernanza de la	1. Revisar que el área de planificación efectuó el relevamiento de la necesidad de automatizar los procesos institucionales sobre la base normativa, misión institucional y necesidad de interoperabilidad, y de forma participativa con los propietarios de los procesos. 2. Revisión de la decisión de aprobación o rechazo sobre la implementación de soluciones de TI. 3. Revisión del modelo de gobierno de TI respecto de su posicionamiento en la estructura organizacional de la Entidad, así como la definición de los roles y responsabilidades para la gestión de TI, tratamiento de riesgos tecnológicos y cumplimiento de los aspectos relacionados con la seguridad de la información.

Organización	
Tema 2 de auditoría: CUMPLIMIENTO DE METAS ¿De qué manera la Dirección conduce y supervisa el cumplimiento de los objetivos y metas de TI de forma periódica?	
Criterios: Se establecen las medidas de desempeño y el Comité de Gobernanza. El Comité de Gobernanza realiza revisiones periódicas y reuniones, y toma las decisiones encaminadas al logro de objetivos y metas planteadas, y existe un sistema de reportes a las partes interesadas y comunica su avance y acciones a tomar.	
Información Requerida Informes periódicos sobre el estado del Plan estratégico de TI y planes operativos de TI. Actas o documentos de revisiones periódicas.	**Método(s) de Análisis** 1. Revisión de los informes del estado de ejecución del Plan estratégico de TI y de los planes Operativos de TI, y otra documentación conexa, para verificar que se cumplan los hitos establecidos en los cronogramas, indicadores y justificativos de las variaciones respecto a los planes aprobados. 2. Revisión de las acciones periódicas adoptadas por el Comité de Gobernanza de TI y que estas hayan sido comunicadas a las partes interesadas, y efectuado el seguimiento a su cumplimiento. 3. Revisar que los planes aprobados cuenten con la asignación de los recursos requeridos para su realización.
Tema 3 de auditoría: Modelo de Gestión de TI ¿Se ha establecido una estructura formal para el funcionamiento del área de TI?	
Criterios: La organización cuenta con una estructura alineada con los requisitos de la entidad que permita planificar, organizar, dirigir, instrumentar, ¿mantener y proveer servicios de manera controlada a los recursos y proyectos de TI?	

Información Requerida	Método(s) de Análisis
Documentación del modelo de TI. Actas con la aprobación de estructura y modificaciones.	1. Verificar que la alta Dirección haya aprobado el modelo de gestión de TI. 2. Verificar que se encuentren definidas las áreas necesarias para de su funcionamiento y atención de los requerimientos de la entidad. 3. Verificar que el modelo describa a alto nivel los procesos de gobierno y gestión de TI para soportar las necesidades de la Entidad.
Tema 4 de auditoría: Código de Ética ¿Se ha establecido un código de ética ca estructura formal para el funcionamiento del área de TI?	
Criterios: La organización cuenta con una estructura alineada con los requisitos de la entidad que permita planificar, organizar, dirigir, instrumentar, ¿mantener y proveer servicios de manera controlada a los recursos y proyectos de TI?	
Información Requerida	**Método(s) de Análisis**
Código de Ética. Actas con la aprobación del Código de Ética.	1. Verificar la existencia de un código de ética aprobado y actualizado que incorpore conductas no aceptables en el ejercicio de las funciones relacionadas con TI. 2. Verificar que se capacitó a las personas en cuanto las conductas no aceptables en el ejercicio de las funciones relacionadas con TI. 3. Verificar que se haya difundido a través de medios establecidos por la entidad el código de ética. 4. Verificar que en contratos con proveedores se incorporen cláusulas relacionadas con ética y probidad en materia de seguridad y confidencialidad de la información. 5. Verificar la existencia de canales de denuncia anónimos para violaciones de aspectos relacionados con TI. 6. Verificar la existencia de registros de incidencia sobre incumplimientos asociadas al uso de los recursos e información de TI. 7. Verificar que se han tomado decisiones relacionadas con los incumplimientos al código de ética que involucren el uso de las tecnologías.
Tema 5 de auditoría: Seguimiento de recomendaciones ¿Se han elaborado los planes de acción producto de las acciones de control?	
Criterios: ¿La entidad ha realizado el registro de los planes de acción para la aplicación de las recomendaciones, y seguimiento a su cumplimiento?	

Información Requerida	Método(s) de Análisis
Planes de acción. Actas con la aprobación de los Planes de acción.	1. Verificar la existencia de Planes de acción. 2. Verificar que se hayan definido y registrado acciones para la totalidad de las recomendaciones. 3. Verificar que las acciones registradas en la plataforma de seguimiento de recomendaciones están alineadas con los hallazgos y recomendaciones de los informes de auditoría. 4. Verifica que las acciones registradas en la plataforma de seguimiento de recomendaciones se hayan ejecutado en los plazos definidos. 5. Verificar que las acciones definidas no excedan los plazos. establecidos por la ley, y en determinadas excepciones que estén motivadas y aprobados, en estos casos debería existir el cronograma para su ejecución.

1.2 Estructuras, normas, políticas y procesos institucionales	
Objetivo de auditoría: garantizar que existan estructuras, normas, políticas, procesos y procedimientos que permitan a la organización cumplir su mandato.	
Tema 6 de auditoría: ¿Es apropiada la estructura del área de TI de la organización para que ésta cumpla los objetivos de TI y satisfaga las necesidades de la institución?	
Criterios: El área de TI se sitúa en un nivel suficientemente alto dentro de la organización, y sus funciones y responsabilidades se definen claramente, incluidas las del Director de Tecnología o Sistemas o su equivalente.	
Información Requerida	**Método(s) de Análisis**
Organigrama general Organigrama de TI Actas de aprobación Políticas y Procedimientos de TI Informes de aseguramiento de la calidad.	1. Revisar los organigramas para determinar que el área de TI esté posicionada a nivel estratégico. 2. Revisar el organigrama de TI para determinar que cuenta con estructura para que responda a los procesos de gobierno y gestión de TI descritos en el modelo de gestión de TI. (ver Manuales de funciones en 1.3). 3. Verificar la conformación y funcionamiento del Comité de Gobernanza de TI, y de los comités de TI adicionales que traten los aspectos operativos (riesgo, seguridad, innovación, cumplimento, calidad, etc.). 4. Verificar que existan las políticas y procedimientos que den cobertura a los procesos de gobierno, gestión y riesgos de TI que se han descrito en el modelo de gestión de TI. 5. Verificar que las políticas y procedimientos de gobierno y

	gestión de TI se encuentren aprobadas, actualizadas y comunicadas. 6. Revisar que se hayan efectuado los informes de aseguramiento de la calidad para los procesos y procedimientos de TI definidos por la entidad, y que incorporen el seguimiento, evaluación y mejora continua.

1.3 Gestión de los Recursos Humanos de TI	
Objetivo de auditoría: Evaluar si se cuenta con suficiente personal calificado / capacitado con acceso a recursos adecuados como para permitir a la organización cumplir con sus objetivos.	
Tema 7 de auditoría: Recursos Humanos y logística ¿Cómo hace la organización para satisfacer las necesidades actuales y futuras de recursos humanos y materiales?	
Criterios: La organización debe contar con un plan para satisfacer sus requerimientos actuales y futuros, para cumplir con las necesidades de la organización.	
Información Requerida	**Método(s) de Análisis**
Políticas organizacionales respecto de: Recursos Humanos Planes y/ programas de capacitación	1. Revisión de las políticas de talento humano para garantizar que están aprobadas y vigentes. 2. Verificar la documentación relacionada con las definiciones de perfiles y requisitos para los cargos en las áreas de TI. 3. Verificar que se hayan cumplido los requisitos de formación y experiencia que se encuentren establecidos en los instrumentos regulatorios. 4. Revisar que se cuente con un programa de capacitación aprobado orientado a las funciones y al desarrollo profesional del personal de las áreas de TI. 5. Revisión del cumplimiento del programa de capacitación dirigido al personal de las áreas de TI. 6. Revisar que sea hayan realizado evaluaciones de desempeño al personal que realiza funciones en las áreas de TI. 7. Revisar que la documentación relacionada con los cargos y funciones mantenga la segregación de funciones. 8. Verifica que en las asignaciones de puestos claves de TI, en caso de ausencias temporal o definitiva cuente con personal que pueda cumplir con esas funciones y responsabilidades.

1.4 Gestión de riesgos de TI	
Tema 8 de auditoría: Gestión de Riesgo ¿De qué manera gestiona la organización sus riesgos de TI?	
Criterios: La organización cuenta con una política y plan de gestión de riesgos, y ha asignado recursos suficientes para identificarlos y gestionarlos.	
Información Requerida	**Método(s) de Análisis**
Política de Gestión de Riesgos de la entidad Política de Gestión de Riesgo de TI Plan de Gestión de Riesgos Lista de riesgos (incluida TI) y estrategias de mitigación. Actas de la evaluación periódica de riesgos u otras reuniones, si están disponibles	1. Evaluar la existencia de la política de gestión de riesgos de la entidad, aprobada y actualizada. 2. Verificar que la política de gestión de riesgos de la entidad releve la importancia de los riesgos asociados al uso y explotación de recursos de TI, así como el perfil de riesgo aceptado por la entidad. 3. Revisar la existencia de la política de gestión de riesgos tecnológicos, verificando que cuente con definiciones metodológicas para la gestión de la identificación y tratamiento de los riesgos de TI. 4. Verificar que se haya realizado periódicamente la evaluación de riesgos de TI acorde al marco metodológico de gestión o de referencia. 5. Verificar que el plan de gestión de riesgos de TI sea consecuencia de la aplicación del marco establecido. 6. Verificar que en el plan de gestión de riesgos de TI se identifican las actividades y responsabilidades. 7. Verificar que se realizaron las actividades correspondientes a la evaluación de riesgos de TI: Identificación, análisis, valoración, tratamiento, y comunicación. 8. Revisar las actas de reunión para garantizar que los nuevos riesgos sean incorporados y analizados según corresponda.

ANEXO 3. DESARROLLO Y ADQUISICIÓN DE TI

MATRIZ SUGERIDA PARA LA AUDITORÍA

2.1 Estudio de factibilidad	
Objetivo de auditoría: Evaluar la suficiencia y eficacia del proceso de análisis de factibilidad, riesgos de proyectos y aseguramiento de cumplimiento legal, técnico y operativo en el desarrollo y adquisición de soluciones tecnológicas en la institución	
Tema 1 de auditoría: ¿Cómo identificar la factibilidad de desarrollo y/o adquisición de soluciones y servicios de TI?	
Criterios: La entidad cuenta con un proceso aprobado para evaluar la viabilidad de las propuestas de desarrollo y adquisición de soluciones tecnológicas.	
Información Requerida	**Método(s) de Análisis**
Propuesta de desarrollo y/o adquisición. Propuesta de contratos y licencias de software. Documentos de política de privacidad y protección de datos. Diagramas de procesos actuales y propuestos. Informe de análisis de impacto de las posibles soluciones. Minutas de reuniones de las partes interesadas. Estudio de costo-beneficio de las propuestas. Presupuestos y cotizaciones de proveedores.	1. Verificar la factibilidad legal, revisando el cumplimiento de las normativas, leyes y regulaciones nacionales e internacionales aplicables; analizar contratos, acuerdos de nivel de servicio (SLA), licencias de software y políticas de protección de datos. 2. Verificar la evaluación de procesos actuales respecto a nuevas soluciones, comparando los flujos de procesos actuales con los propuestos y analizar los posibles impactos operativos, financieros y ambientales; solicitando los diagramas de procesos, matrices de impacto y actas de reuniones donde se discutan los cambios. 3. Verificar que el análisis de costo-beneficio, contenga el estudio de otras alternativas y fue la más beneficiosa tomando consideración su compatibilidad, escalabilidad, sostenibilidad y costos de mantenimiento y de operación en el tiempo, que justifiquen su selección. 4. Verificar que se relevaron las necesidades de seguridad como el control de acceso y configuraciones de la solución tecnológica para garantizar la integridad, disponibilidad y confidencialidad de la información. 5. Verificar la matriz de riesgos y plan de acción, revisando que se hayan identificado los riesgos relevantes, su valoración, acciones de mitigación y seguimiento de acciones correctivas. 6. Verificar la factibilidad técnica y compatibilidad tecnológica, evaluando la arquitectura propuesta y su integración a la infraestructura y plataforma tecnológica existente, que incluya análisis de la capacidad de los

Comparativos de soluciones alternativas. Matriz de riesgos y evaluaciones periódicas. Planes de acción y seguimiento Informes de reuniones del comité de riesgos. Diagramas de arquitectura tecnológica. Resultados de pruebas de interoperabilidad. Informes de compatibilidad y evaluación técnica. Informes de evaluación de sistemas actuales. Estudios comparativos de soluciones alternativas. Justificaciones y recomendaciones de la comisión técnica o comité de adquisiciones/compras	recursos tecnológicos. 7. Verificar que se definieron interfaces con los criterios y estructura de datos para el intercambio de información a través de los servicios de interoperabilidad y su compatibilidad con la solución propuesta. 8. Determinar si se puede alcanzar una solución con sistemas existentes o evaluar alternativas, revisando reportes de evaluación de sistemas actuales y análisis de alternativas tecnológicas con la participación de las partes interesadas; analizando los informes de uso y capacidad de sistemas existentes y capacidad requerida, así como su vigencia tecnológica y comparativos con nuevas soluciones.

<table>
<tr><th colspan="2">2.2 Desarrollo y gestión de requisitos</th></tr>
<tr><td colspan="2">Objetivo de auditoría: Evaluar de qué manera la entidad identifica, prioriza y gestiona sus requerimientos de TI.</td></tr>
<tr><td colspan="2">Tema 2 de auditoría:
¿Cómo identifica la entidad las necesidades de los usuarios de los servicios de TI?</td></tr>
<tr><td colspan="2">Criterios:
La entidad cuenta con un plan o procedimiento aprobado sobre la forma de identificar las soluciones y analizar los requisitos antes de su adquisición o construcción para asegurarse de que se ajustan a los requisitos estratégicos de la entidad cubriendo los procesos, aplicaciones, información/datos, infraestructura y servicios de la institución.</td></tr>
<tr><td>Información Requerida</td><td>Método(s) de Análisis</td></tr>
<tr><td>Actas de reuniones, listas de requerimientos, historias de usuario y diagramas de flujo.

Registros de los controles de cambio aplicados

Informes de pruebas de validación funcional, certificados de cumplimiento normativo y documentación de homologación

Actas de aceptación, reportes de resultados de pruebas y documentos que acrediten la aprobación formal.

Inventarios actualizados de activos de TI, informes de compatibilidad, y evidencia de que la</td><td>1. Verificar que el procedimiento o plan aprobado para el desarrollo y gestión de requerimientos establezca las actividades, responsables, entregables y niveles de autorización para el levantamiento y análisis de necesidades y requerimientos para la adquisición o construcción de soluciones, considerando la normativa aplicable y criterios de seguridad.
2. Revisar los registros generados durante el levantamiento de necesidades, como actas de reuniones, listas de requerimientos, historias de usuario y diagramas de flujo; solicitar evidencias formales que respalden la recopilación de expectativas, restricciones y requisitos funcionales, no funcionales y normativos, asegurando la trazabilidad, con la validación y aceptación de las partes interesadas de cada requerimiento desde su origen hasta su implementación.
3. Verificar el proceso de levantamiento y control de cambios, revisando la documentación utilizada en la identificación de necesidades, tales como listas validadas de requerimientos aprobados y casos de uso formalizados por las partes interesadas; además, solicitar los registros de los controles de cambio aplicados, como bitácoras de modificaciones o matrices de seguimiento, que permitan evidenciar la gestión sistemática de las actualizaciones.
4. Evaluar el cumplimiento normativo y funcional, comprobar que el sistema o aplicativo desarrollado cumple tanto con los requerimientos funcionales definidos como con las normativas vigentes que regulan los procesos automatizados; para ello, solicitar informes de pruebas de validación funcional y de parametrización, así como realizar</td></tr>
</table>

solución tecnológica propuesta se integra adecuadamente con los sistemas y recursos ya disponibles. Acuerdos de niveles de servicio (SLA), manuales de soporte, contratos de mantenimiento y registros de incidencias resueltas. Bitácoras, registros de gestión de versiones y documentación de los cambios. Informe de validación de datos migrados y registros de incidencias detectadas y solucionadas Convenios de confidencialidad firmados Resultados de pruebas de rendimiento, reportes de seguridad y documentación técnica que respalde el cumplimiento de estos indicadores.	comprobaciones y pruebas. 5. Revisar la participación de las áreas clave en las pruebas de validación y aceptación y la transición a producción del sistema; solicitar evidencias como actas de aceptación, reportes de resultados de pruebas y documentos que acrediten la aprobación formal de las partes interesadas involucradas, asegurando así la transparencia y conformidad en el proceso. 6. Validar el uso y compatibilidad de activos de TI, verificando que los activos de tecnología existentes han sido considerados y reutilizados de manera eficiente; requerir inventarios actualizados de activos de TI, informes de pruebas de funcionamiento, compatibilidad, que evidencie que la solución tecnológica propuesta integra adecuadamente los sistemas y recursos ya disponibles. 7. Verificar que se garantiza la interoperabilidad mediante la comprobación de que se han efectuado el análisis de pruebas de integración y documentación técnica que certifique la comunicación efectiva entre sistemas internos y externos; solicitar reportes de pruebas de interoperabilidad, acuerdos formales de integración y descripciones técnicas de interfaces. 8. Revisar condiciones de soporte y mantenimiento, confirmando que se han definido y documentado claramente las condiciones para el soporte y mantenimiento de los sistemas; solicitar los acuerdos de niveles de servicio (SLA), manuales de soporte, contratos de mantenimiento y registros de incidencias y problemas resueltos e informes técnicos de su monitoreo y de cumplimiento. 9. Verificar registro histórico de versiones, revisando las bitácoras y bibliotecas, registros de gestión de versiones y documentación de los cambios implementados a lo largo del ciclo de vida del software. 10. Cuando corresponda, se debe inspeccionar la correcta ejecución de procesos de migración de datos; solicitar planes de migración, reportes de resultados, evidencias de validación de datos migrados y registros de incidencias detectadas y solucionadas durante el proceso. 11. Comprobación de acuerdos de confidencialidad, revisando los acuerdos y convenios suscritos por las partes involucradas, así como su mantenimiento y custodia.

	12. Verificar que se definieron y aplicaron criterios de evaluación, parámetros de medición para las pruebas de rendimiento, seguridad y disponibilidad, constatando que se han cumplido los parámetros establecidos en cuanto a tiempos de respuesta, cifrado de datos y disponibilidad del sistema, solicitando los resultados de pruebas de rendimiento, reportes de seguridad y documentación técnica que respalde el cumplimiento de estos indicadores.

2.3 Gestión y control de proyectos	
Objetivo de auditoría: Evaluar de qué manera la entidad gestiona y controla el desarrollo o la adquisición de proyectos de TI.	
Tema 3 de auditoría: **¿Cómo planifica la entidad el desarrollo o la adquisición de proyectos de TI?**	
Criterios: La entidad cuenta con un plan de gestión de proyectos o su equivalente para cada proyecto que guie su ejecución.	
Información Requerida	**Método(s) de Análisis**
Plan de gestión de proyectos o equivalente Proyectos de TI Cronogramas de Ejecución Control del Cambios al Proyecto de TI Comunicaciones de seguimiento Informe de cierre de proyectos	1. Revisar los documentos del proyecto de TI, verificando que contengan la descripción del proyecto, alcance, objetivos, con la identificación de las partes interesadas (internas o externas), costo, cronograma, riesgos y estructura de la gestión del proyecto entre otros. 2. Verificar que los cambios al proyecto de TI hayan sido documentados y aprobados por los niveles correspondientes, comprobando que los documentos del proyecto hayan sido actualizados conforme las modificaciones autorizadas ya sea al alcance, plazos, presupuesto, funcionalidades, recursos y otras definiciones. 3. Revisar que los cambios al proyecto de TI cuenten con el análisis de su impacto y que estos fueron comunicado formalmente a las partes interesadas. 4. Verificar que el proyecto de TI cuente con mecanismos de control para la gestión de riesgos, seguimiento, comunicación y atención de medidas correctivas. 5. Revisar que durante la ejecución del proyecto de TI se hayan emitido informes de avance que incluyan entre otros aspectos, la evaluación del estado actual, las actividades

	realizadas, en ejecución y pendientes y reporte de novedades y compromisos de sus ejecutores y partes interesadas. 6. Verificar que exista documentación del cierre del proyecto de TI que incluya la validación del cumplimiento de los hitos y entrega de productos con la aceptación de los responsables de su aprobación, con las lecciones aprendidas y de mejora para futuros proyectos.

2.4 Diseño/Desarrollo de sistemas y aplicaciones de software	
Objetivo de auditoría: Evaluar de qué manera la entidad garantiza que las actividades relacionadas con la construcción de sistemas consideran los requisitos de la ingeniería de software y buenas prácticas para el desarrollo de soluciones.	
Tema 4 de auditoría: Diseño de soluciones de Software **¿Se realizan actividades de diseño en el desarrollo de software en base a algún modelo de Ciclo de Vida de Desarrollo del Software (SLDC)?**	
Criterios: La entidad cuenta con un proceso para desarrollar y documentar diseños para la solución tecnológica, procesos de negocio y flujos de trabajo. Usar técnicas de desarrollo por fases o metodologías ágiles definidas. Se asegura la alineación con la estrategia de TI y la arquitectura institucional. Se reevalúan y actualizan los diseños cuando se presentan problemas significativos durante las fases de diseño detallado o construcción, o según evolucione la solución. Se aplican enfoques centrado en el usuario; asegurándose de que las partes interesadas participan activamente en el diseño y la aprobación de cada versión.	
Información requerida	**Método(s) de Análisis**
Documento de requerimientos funcionales y no funcionales aprobados. Diagramas de arquitectura y diagramas de componentes técnicos. Manuales técnicos y especificaciones de diseño detallado. Matrices de trazabilidad de requisitos. Prototipos de pantallas e informes, mockups o wireframes. Actas de comités de	1. Verificar si la entidad definió la arquitectura de datos que establece como se recopila, almacena, integra, acceden y gobiernan los datos dentro de la institución con la que revisará que los desarrollos y mantenimientos de las soluciones de software se encuentre alineado a estas definiciones, así como los requerimientos funcionales para su desarrollo interno o adquirido. 2. Verificar que como parte de la arquitectura se haya definido los componentes tecnológicos de acuerdo con la normativa vigente y alineados a los requerimientos funcionales aprobados, revisando las especificaciones de diseño, diagramas de arquitectura, manuales técnicos y actas de validación de requisitos; como evidencia, buscar versiones aprobadas, matrices de trazabilidad y registros de revisión técnica.

arquitectura, actas de validación y minutas de reuniones técnicas. Análisis de integración y compatibilidad, contratos de interoperabilidad. Fichas técnicas de infraestructura y dimensionamiento. Catálogos de requisitos de seguridad y conectividad. Planes de escalabilidad, análisis de capacidad y documentación de API´s o arquitecturas SOA. Reportes de pruebas de integración o interoperabilidad.	3. Verificar el desglose de los componentes de la arquitectura, asegurando que incluya la descripción detallada de módulos del sistema o aplicativo, software base, bases de datos, lenguajes de programación y la infraestructura tecnológica con la capacidad de recursos requeridos; para ello, se revisarán diagramas de componentes, documentos de diseño técnico y actas de reuniones de arquitectura, validados y aprobados. 4. Verificar la identificación y descripción de entradas, procesamientos y salidas, asegurando que estén representadas mediante diseños de pantalla e informes, coherentes con los requisitos levantados y aprobados para la construcción del sistema o aplicativo; para ello, se revisan prototipos de interfaz de usuario, diseños de reportes, diagramas de flujo y documentación funcional; como evidencia, buscar prototipos validados, actas de talleres y registros de aceptación de usuarios clave. 5. Verificar la inclusión de servicios externos en el diseño y arquitectura, confirmando que se haya considerado la interoperabilidad con fuentes externas y el análisis de compatibilidad con los servicios tecnológicos existentes, para asegurar la integración con la solución tecnológica propuesta; para ello, se revisan documentos de análisis de integración, acuerdos de interoperabilidad, diagramas de interoperabilidad y documentación técnica para la interconexión, contratos de servicios y manuales de interfaces. 6. Verificar que la arquitectura contemple las especificaciones técnicas de los equipos, aplicativos de seguridad y servicios de conectividad necesarios para el funcionamiento, despliegue y operación de la solución tecnológica; para ello, revisará las características técnicas del equipamiento, licenciamiento de software base, de seguridad y conectividad, con los respectivos justificativos técnicos de su necesidad para el funcionamiento de la solución. 7. Verificar el diseño de escalabilidad e interoperabilidad, confirmando que el diseño del software incorpora la escalabilidad, es decir, la capacidad de ajustarse a nuevas necesidades y crecimiento de la demanda; y que asegura la interoperabilidad para compartir información con otros sistemas y servicios externos; para ello, se revisan planes de

	crecimiento, análisis de capacidad, arquitecturas orientadas a servicios (SOA) o API´s documentadas, y manuales de integración. 8. Verificar en los contratos para el desarrollo e implementación de software, la existencia de cláusulas que obliguen al contratista a la entrega de forma íntegra del código fuente en su última versión probada e instalada en el ambiente de producción y entregada a conformidad de la entidad; así como las modificaciones y actualizaciones de las versiones de la solución durante el periodo de soporte y mantenimiento, para su uso sin restricción. 9. Verificar que se realizó el trámite administrativo para el registro de la propiedad intelectual y derechos de autor a nombre de la Entidad ante el organismo competente, de las soluciones tecnológicas desarrolladas internamente o adquiridas.
Tema 5 de auditoría: Desarrollo de soluciones **¿Se realizan actividades de construcción de software en base a algún modelo de Ciclo de Vida de Desarrollo del Software (SLDC)?**	
Criterios: La entidad desarrolla progresivamente los componentes de la solución en un entorno independiente, de acuerdo con los diseños detallados siguiendo estándares y requisitos de desarrollo y documentación, de aseguramiento de la calidad (QA) y de aprobación. Se asegura incluir todos los requisitos de control en los procesos institucionales, las aplicaciones y los servicios de infraestructura soportadas por TI, servicios y productos de tecnología, así como, servicios de proveedores y de otras entidades.	
Información requerida	**Método(s) de Análisis**
Documento final de requerimientos funcionales y no funcionales aprobados. Entregables de desarrollo, versiones finales de software. Manuales de codificación, estándares y procedimientos de desarrollo aprobados. Repositorios de versiones y control de cambios. Bitácoras de incidencias y	1. Verificar que la construcción de los sistemas o aplicaciones cumplió con los requerimientos funcionales y no funcionales aprobados; para ello, se revisan los entregables de desarrollo tales como: listas validadas de requerimientos aprobados y casos de uso formalizados por las partes interesadas; resultados de pruebas unitarias e integrales, actas de aceptación de usuarios y matrices de cumplimiento de requisitos; así como, realizar comprobaciones y pruebas. 2. Verificar que la codificación y desarrollo de programas y documentos utilizó las metodologías, estándares y procedimientos aprobados, incluyendo validaciones generales y específicas de aplicación; para ello, revisar manuales de codificación, guías de estilo, y documentos de

reportes de resolución de bugs. Planes de pruebas, resultados de pruebas unitarias, integrales y de aceptación. Actas de paso a producción y autorizaciones de migración. Programas y temarios de capacitación técnica y funcional. Actas de asistencia y registros de participación. Certificados de capacitación y evaluaciones de conocimiento.	revisiones de calidad del código fuente; así como, realizar a través de muestreo la validación de la aplicación de estándares en el código fuente. 3. Verificar que se documentaron las modificaciones a los sistemas o aplicativos, y que estas contribuyeron con correctivos o mejoras funcionales en aplicación a los requerimientos funcionales; para lo cual, se revisan registros de control de versiones, bitácoras de cambios, reportes de incidencias y documentación técnica de ajustes y requerimientos funcionales de mejora o tickets de incidentes y documentos de aprobación de mejoras y/o solución de incidentes, pruebas y del paso a producción. 4. Verificar que se cumplió con las pruebas y procedimientos establecidos para la implantación del nuevo sistema, incluyendo aspectos de seguridades, bases de datos, conectividad y configuración, y que se documentó el paso a producción; para ello, se revisan planes de pruebas que incluyan validaciones funcionales, controles de aplicación, seguridad, rendimiento y de integración; informes de resultados de pruebas, checklists con los criterios de aseguramiento, actas de despliegue y paso a producción con la documentación de aceptación de las partes interesadas, en caso de existir migración de datos, obtener documentación del plan de migración, y resultados de su ejecución con la documentación de respaldo, a finde garantizar la integridad y exactitud de los datos; así como, realizar comprobaciones y pruebas. 5. Verificar la capacitación al personal técnico encargado de soporte y mantenimiento, confirmando que se haya realizado con el contenido a fin a la solución tecnológica para garantizar la sostenibilidad operativa; para lo cual, solicitar y revisar programas de capacitación, listas de asistencia, temarios y evaluaciones de conocimiento; actas de asistencia, certificados internos y registros de evaluación de habilidades. 6. Verificar la documentación de la capacitación a usuarios funcionales en el uso del nuevo sistema, confirmando la existencia de manuales de usuario, temarios, actas de asistencia y, de ser el caso, certificados de asistencia o aprobación; para ello, se revisan cronogramas de inducción, materiales de formación y registros de participación; como

	evidencia, buscar temarios aprobados, listas firmadas de asistentes y constancias emitidas.

2.5 Aseguramiento de la Calidad y Pruebas	
Objetivo de auditoría: Evaluar de qué manera la organización garantiza que los proyectos de desarrollo o adquisición de TI cumplen con los objetivos de calidad.	
Tema 6 de auditoría: QA Técnico al desarrollo de software ¿Cuenta la organización con una estructura de aseguramiento de la calidad y están definidas sus funciones y responsabilidades; o en su defecto se establecieron procedimientos en el cual se describen los responsables técnicos y funcionales para el aseguramiento y pruebas?	
Criterios: Un procedimiento establecido para la conducción de actividades de aseguramiento de la calidad.	
Información requerida	**Método(s) de Análisis**
Plan general de pruebas aprobado y cronograma de ejecución. Matrices de casos de prueba y registros de guías de ejecución. Bitácoras de pruebas, formularios de resultados y evidencias de ejecución. Matrices de requisitos funcionales, no funcionales y de seguridad. Reportes de validación normativa y listados de verificación. Reportes de defectos, bitácoras de incidencias y actas de cierre de problemas.	1. Verificar que el plan de pruebas comprenda todas las funcionalidades previstas, los responsables designados y los tiempos definidos para su realización, asegurando que el cronograma y alcance de las pruebas se encuentren aprobados; para lo cual, se deberá revisar planes de pruebas, cronogramas y actas de validación con la aceptación de sus responsables. 2. Verificar que la documentación de las pruebas incluya el detalle de cada funcionalidad evaluada, los datos de prueba utilizados, los reportes de resultados, los responsables de ejecución y las firmas de responsabilidad que respalden la revisión; para ello, se revisarán bitácoras de pruebas, formularios de registro, informes de resultados y actas de cierre de pruebas. 3. Verificar que las pruebas contemplen la revisión de la normativa y los procedimientos relacionados con el alcance y objetivos de la solución, así como el cumplimiento de los requerimientos funcionales, no funcionales y de seguridad de la información definidos para el proyecto; para ello, se revisan matrices de requisitos, normativa relacionada con la solución tecnológica y reportes de su validación. 4. Verificar que el plan y la batería de pruebas incluyan los casos específicos a evaluar, los actores involucrados, los datos de entrada y los resultados esperados, asegurando

Planes y resultados de pruebas de integración. Planes de recuperación, reportes de pruebas de recuperación y seguridad. Firmas de responsables de ejecución, revisión y aprobación de resultados.	que exista documentación de respaldo que evidencie la ejecución de cada caso; para ello, se revisan matrices de casos de prueba, guías de ejecución y evidencias de resultados. 5. Verificar la resolución de los problemas encontrados como resultado de la aplicación de las pruebas, confirmando que se registraron incidencias, se documentaron las acciones correctivas y se cerraron adecuadamente; para ello, se revisan reportes de defectos, bitácoras de seguimiento y actas de cierre de incidencias con los informes correspondientes. 6. Verificar la existencia de pruebas de integración, confirmando que se hayan planificado y ejecutado para validar la interoperabilidad entre los componentes del sistema y con servicios externos; para ello, se revisan planes de pruebas de integración, resultados de ejecución y actas de validación y aceptación. 7. Verificar las pruebas de recuperación y de seguridad, confirmando que se hayan realizado según lo planificado y que existan resultados documentados con las firmas de responsabilidad de elaboración, revisión y aprobación; para ello, se revisan planes de contingencia, resultados de pruebas de recuperación, reportes de pruebas de seguridad y actas de aprobación.

2.6 Gestión de la Configuración	
Objetivo de auditoría: Evaluar de qué manera la Entidad gestiona la configuración de los productos relacionados con el desarrollo y la adquisición.	
Tema 7 de auditoría: **¿Se cuenta con un registro de ítems de configuración (CI) que permita controlar el estado de los parámetros de los elementos de componentes críticos de TI?**	
Criterios: La entidad establece y mantiene un modelo lógico de servicios, activos, infraestructura, y registro de los elementos de configuración (CI), incluyendo las relaciones entre estos; incluye los CI´s que se consideran necesarios para gestionar los servicios eficazmente y, proporcionar una única descripción confiable de los activos en un servicio.	
Información Requerida	**Método(s) de Análisis**
Plan de gestión de la configuración y	1. Verificar que el plan de gestión de la configuración esté alineado con la infraestructura de TI, que contemple todos

matrices de alineación técnica. Base de datos de configuración (CMDB) y listados de activos actualizados. Informes de inventario físico y reportes de conciliación de activos. Logs de auditoría de configuración y bitácoras de cambios. Procedimientos de configuración y listas de verificación de paso a producción. Registros de versiones de sistemas y respaldos históricos. Matrices de roles y responsabilidades, registros de acceso y permisos. Informes de auditoría técnica sobre configuración y hallazgos de cumplimiento. Actas de revisión y evidencias de planes de acción correctiva.	los elementos necesarios para controlar, registrar y mantener la coherencia técnica de componentes y servicios; para ello, se revisan planes de configuración, identificación de roles y responsabilidades, detalle de los elementos y componentes de TI y su relación con los servicios tecnológicos provistos por la Unidad de TI (matriz de alineación) y actas de validación de los elementos relacionados con los cambios realizados a la configuración. 2. Validar que el registro o base de datos de configuración contenga información completa y actualizada de todos los componentes relevantes, incluyendo software, hardware, documentación técnica y versiones implantadas; para ello, se revisan bases de datos de configuración (CMDB), listados de activos y fichas técnicas; como evidencia, buscar reportes de configuración actualizados y registros de revisión periódica. 3. Contrastar el registro o base de datos de configuración con los activos existentes de la entidad, a fin de documentar las diferencias detectadas y asegurar la coherencia entre el inventario físico y el inventario lógico; para ello, se revisan informes de inventario, registros de inspección física y reportes de constatación de activos. 4. Verificar la existencia de la trazabilidad y registros de cambios (logs de auditoría) en los procedimientos utilizados para agregar, modificar o eliminar elementos de configuración, garantizando que todo cambio esté registrado y validado; para ello, se revisan logs de auditoría, bitácoras de cambios y matrices de control de configuración. 5. Verificar si se aplicaron los procedimientos establecidos para la configuración de los sistemas e infraestructura requerida para su puesta en producción, y que se encuentren documentados los resultados obtenidos; para ello, se revisan procedimientos operativos, listas de verificación de configuración y reportes de implementación; actas de paso a producción, checklists firmados y reportes de validación técnica. 6. Verificar que se mantienen y respaldan cronológicamente las versiones de los sistemas y configuraciones, de modo tal que la entidad esté en condiciones de volver a versiones conocidas y probadas si fuese necesario; para ello, se revisan

	historiales de versiones, repositorios de control y bitácoras de cambios; como evidencia, buscar registros de versiones, respaldos almacenados y reportes de recuperación de versiones. 7. Verificar la habilitación y temporalidad de los accesos de acuerdo con los roles y responsabilidades requeridos para la administración y funcionamiento de los sistemas, asegurando que se cumpla la segregación de ambientes de TI; para ello, se revisan matrices de roles, registros de permisos y logs de acceso; como evidencia, buscar listados de usuarios, reportes de auditoría de acceso y autorizaciones firmadas. 8. Verificar los informes de auditoría de la configuración, confirmando que permitan evaluar la aplicación de estándares, políticas y procedimientos establecidos en los cambios efectuados a la configuración; para ello, se revisan reportes de auditoría técnica, actas de revisión y matrices de cumplimiento; identificar hallazgos de auditoría y planes de acción correctiva.

2.7 Adquisición de Infraestructura tecnológica	
Objetivo de auditoría: Evaluar de qué manera la Entidad gestiona la configuración de los productos relacionados con el desarrollo y la adquisición.	
Tema 8 de auditoría: **¿Los procedimientos de adquisición de infraestructura, a más de lo requerido por la normativa de contratación pública, detallan actividades que fundamentan solicitudes basadas en análisis de las capacidades y demanda futura?, ¿Se cuenta con un inventario actualizado de bienes tecnológicos?**	
Criterios: Las actividades de gestión de adquisición se realizan de acuerdo con la normativa legal e interna vigente, procurando que las dotaciones estén basadas en necesidades reales y una planificación de la demanda.	
Información Requerida	**Método(s) de Análisis**
Especificaciones técnicas y funcionales aprobadas. Estudios de capacidad	1. Revisar que los requerimientos técnicos y funcionales fueron definidos y documentados con el análisis pertinente de las áreas de TI, funcionales y/o usuarias, debidamente suscritos antes de la adquisición; para ello, se revisan documentos de especificaciones, actas de validación y autorizaciones de

instalada, demanda y análisis costo-beneficio. Informes de tomas físicas e inventarios patrimoniales. Estudios de ingeniería, diseños técnicos y dictámenes de factibilidad. Expedientes de contratación y resoluciones administrativas. Certificaciones de proveedores y autorizaciones de fabricante. Contratos suscritos con cláusulas SLA, garantías y PI. Actas de entrega-recepción y reportes de conformidad. Registros de inventario y sistemas contables actualizados. Planes y resultados de pruebas de integración y compatibilidad. Planes de mantenimiento, registros de renovación	requerimientos; como evidencia, buscar requerimientos firmados, actas de reuniones técnicas y registros de aprobación. 2. Confirmar que las adquisiciones de soluciones tecnológicas se basen en un análisis de la capacidad instalada frente a la capacidad utilizada, contrastado con un análisis de demanda que justifique la relación costo-beneficio; para ello, se revisan estudios de capacidad, proyecciones de demanda y reportes de análisis de la mejora de los servicios asociados a la infraestructura de TI. 3. Verificar los informes de las tomas físicas de los bienes tecnológicos efectuadas conforme la normativa vigente, asegurando que coincidan con los registros contables y de activos de la entidad; para ello, se revisan actas de inventario y constatación física y reportes de control de activos y registros contables. 4. Verificar que la entidad contó con los estudios y diseños completos necesarios para la adquisición de infraestructura de TI, asegurando que estos documentos contemplen la viabilidad técnica y presupuestaria; para ello, se revisan estudios de ingeniería, diseños técnicos y dictámenes de factibilidad. 5. Verificar que se cumplió con las disposiciones normativas de contratación vigentes para la adquisición de infraestructura de TI, garantizando que se hayan seguido los procedimientos legales establecidos; para ello, se revisan expedientes de contratación, resoluciones administrativas, así como, comprobar la aplicación de la normativa en los procesos de contratación. 6. Verificar el análisis de la capacidad del proveedor en relación con la comercialización de infraestructura de TI, confirmando que esté autorizado por el fabricante y cuente con servicios de mantenimiento y soporte certificados; para ello, se revisan certificaciones de proveedor, registros de autorización de fabricante y contratos de soporte, así como, certificado de las actividades comerciales emitido por la entidad que controla la aplicación de la política tributaria. 7. Verificar que los contratos suscritos incluyan cláusulas claras sobre niveles de servicio (SLA), soporte técnico, garantías, propiedad intelectual y mantenimiento, asegurando que este último garantice la vigencia tecnológica; para ello, se

y actas de baja.	revisan contratos firmados, anexos y cláusulas técnicas relacionadas con los servicios de soporte y mantenimiento, certificaciones emitidas por el fabricante para los servicios post implementación y garantía de los bienes. 8. Verificar que los bienes y/o servicios adquiridos de TI fueron entregados conforme a lo estipulado en las cláusulas contractuales, dejando constancia mediante actas de entrega-recepción suscritas por los representantes legales de la entidad y del proveedor o sus delegados; para ello, se revisan actas de entrega-recepción conforme las condiciones establecidas en la normativa de contratación pública, cronogramas de entrega y registros de conformidad, con el respaldo de informes técnicos. 9. Verificar que los bienes y/o servicios adquiridos de TI se encuentran registrados como activos de la entidad, asegurando su incorporación en los sistemas contables y patrimoniales; para ello, se revisan registros de inventario, informes de constatación y registros contables. 10. Verificar que los bienes y/o servicios adquiridos de TI se integraron con los sistemas existentes, validando compatibilidad, rendimiento y seguridad mediante pruebas realizadas antes de la puesta en producción; para ello, se revisan planes de pruebas de integración, informes con los resultados y actas de validación, así como, validar reportes de monitoreo y disponibilidad. 11. Verificar la existencia de documentación sobre el mantenimiento, renovación y baja de activos para los componentes de hardware y software de la infraestructura de TI, asegurando que se mantenga el control y la trazabilidad de su ciclo de vida; para ello, se revisan planes de mantenimiento, registros de renovación y actas de baja de activos; informes de mantenimiento, reportes de renovación y documentación de los trámites administrativos para la baja bienes.

ANEXO 4. OPERACIONES DE TI

MATRIZ SUGERIDA PARA LA AUDITORÍA

3.1 Gestión de la Capacidad	
Objetivo de auditoría: Evaluar si el área de TI garantiza que la capacidad y el desempeño de los sistemas informáticos y recursos tecnológicos satisfacen las necesidades actuales y futuras del negocio.	
Tema 1 de auditoría: Acuerdo en relación con los parámetros de funcionamiento ¿Existe un acuerdo documentado entre la entidad y el área de TI que se utilice como base para la selección de parámetros de funcionamiento de las operaciones de TI?	
Criterios: El área de TI declara acuerdos de funcionamiento para la alineación de la capacidad de los servicios con las necesidades y expectativas del negocio, en base a Acuerdos de Nivel de Servicio operativos internos (OLA); esto implica asegurar que los recursos de TI estén disponibles y sean suficientes para cumplir con los requisitos de rendimiento y disponibilidad especificados en los SLA.	
Información requerida	**Métodos de Análisis**
SLA interno, o cualquier otra forma de acuerdo Parámetros de funcionamiento de TI Reportes de desempeños de ítems de servicio	1. Revisión del acuerdo o la guía de funcionamiento que el área de TI está utilizando. Garantizar que ha sido revisado y firmado por los usuarios del negocio pertinentes o por la dirección ejecutiva. 2. Comparación del desempeño de ítems de servicios (por ejemplo: disponibilidad de recursos, el tiempo de respuesta del servidor central), con lo obtenido por los responsables de los procesos del negocio para verificar que el área de TI cumple con la guía de funcionamiento.
Tema 2 de auditoría: Monitoreo de la capacidad ¿El área de TI recopila o revisa en tiempo real o periódicamente los datos de desempeño del sistema para mejorar sus alineamientos con las necesidades del negocio?	
Criterios: Buenas prácticas de los administradores de los sistemas o las redes incluida la base de referencia para el desempeño, recolección de información relacionada con el tráfico y la configuración, disponibilidad de recursos del sistema, observación de estadísticas y tendencias del tráfico, análisis hipotéticos y utilización de herramientas para identificar las causas del deterioro del desempeño.	
Información Requerida	**Métodos de Análisis**
Informes, medidas a tomar, tiempo de respuesta de la mesa de servicios, y otros parámetros.	1. Verificar reportes de monitoreo periódico del rendimiento de los sistemas y recursos tecnológicos para detectar posibles cuellos de botella o sobrecargas, asegurando que se tomen medidas

Registros de ciclo de vida de activos y manuales de gestión. Inventarios actualizados y listas de clasificación por tipo y criticidad. Etiquetas de identificación y reportes de control físico. Planes de mantenimiento, bitácoras de soporte y reportes de intervención. Actas de entrega-recepción y registros de custodia de activos. Informes de verificaciones periódicas y conciliaciones contables. Inventarios de licencias de software y reportes de estado. Contratos de adquisición, mantenimiento, soporte y garantías. Políticas de eliminación segura, bitácoras de borrado y certificados de destrucción. Registros de movimientos y actas de baja de activos.	proactivas para mantener la capacidad adecuada; para ello, se revisan reportes de desempeño, dashboards de monitoreo y bitácoras de análisis; como evidencia, buscar reportes históricos de rendimiento, alertas generadas y registros de acciones correctivas. 2. Verificar la existencia de documentación que permita identificar, analizar y resolver problemas relacionados con la falta de disponibilidad o insuficiencia de recursos tecnológicos, garantizando la continuidad operativa; para ello, se revisan procedimientos de gestión de capacidad, registros de incidentes y planes de acción; como evidencia, buscar reportes de problemas, bitácoras de análisis y registros de soluciones implementadas. 3. Constatar que en los casos donde la capacidad esté sujeta a servicios provistos por terceros, se cumplieron los acuerdos contractuales establecidos y se verificó periódicamente que la capacidad contratada corresponda con la demanda real, permitiendo ajustes correctivos oportunos; para ello, se revisan contratos de servicio, reportes de cumplimiento de SLA y registros de validación; como evidencia, buscar contratos vigentes, reportes de desempeño de proveedores y actas de seguimiento de capacidad. 4. Revisar el acuerdo o la guía de funcionamiento que el grupo de TI esté utilizando para gestionar la capacidad de los sistemas, asegurando que se mantenga alineada a las mejores prácticas (p. ejemplo ITIL) y las necesidades de la entidad; para ello, se revisan acuerdos operativos, guías internas y manuales de procedimiento; como evidencia, buscar documentos aprobados, versiones actualizadas y registros de capacitación. 5. Comparar el desempeño real del servicio con los parámetros de referencia establecidos, verificando que se evalúe periódicamente el nivel de cumplimiento y se ajusten las proyecciones de capacidad; para ello, se revisan métricas de rendimiento, indicadores clave (KPIs) y reportes comparativos; como evidencia, buscar gráficos de desempeño, reportes de comparación y registros de revisión de metas.

	6. En general, revisar los elementos que podrían tener impacto en la capacidad, es decir, comparar los parámetros reales de capacidad con los requerimientos del SLA, etc.
Tema 3 de auditoría: Análisis de los datos de desempeño ¿Se analizan y ajustan los datos de desempeño para mejorar la eficiencia y evitar limitaciones en la capacidad? Si fuese necesario, ¿ha planificado y adquirido el área de TI recursos adicionales para satisfacer las necesidades del negocio? ¿El área de TI emplea, capacita o contrata personal conforme cambian las necesidades de la organización?	
Criterios: Parámetros establecidos en el acuerdo o guía de operaciones, buenas prácticas para la optimización del desempeño (memoria, optimización del tiempo de respuesta de la red, sistema operativo, I/O, diseño eficiente del esquema de la base de datos, programación de tareas según la prioridad y el requerimiento de recursos, procedimientos de actualización o ajuste establecidos para manejar los problemas de capacidad tanto sobre una base reactiva como a largo plazo).	
Información requerida Informes, acciones, gráficos de parámetros de desempeño Actas de las reuniones de la Gerencia del área de TI	**Métodos de Análisis** 1. Revisión de los informes que el área de TI genera diariamente o en otro período de tiempo elegido, verificar si genera y analiza datos sobre tendencias, identifica los impedimentos para tomar medidas, informes de excepción para los problemas de capacidad. Comparación con los requerimientos del SLA. 2. Comparación de informes y patrones de tendencia para verificar las medidas procesales adoptadas en respuesta a los informes. 3. Revisión de las actas de las reuniones y verificación sobre si las cuestiones relacionadas a la dotación del personal de TI, los problemas de capacidad y cualquier necesidad adicional de recursos se discuten y destacan en el momento adecuado.

<table>
<tr><td colspan="2">3.2 Gestión de Cambios</td></tr>
<tr><td colspan="2">Objetivo de auditoría: Evaluar si la entidad ha implementado un procedimiento estandarizado para el control de
cambios en los sistemas y aplicaciones claves de TI.</td></tr>
<tr><td colspan="2">Tema 4 de auditoría: Políticas y/o Procedimientos de gestión de cambios
¿Cuenta la organización con una política y/o procedimientos aprobados de gestión de cambios que contenga los controles apropiados en todo el ciclo?</td></tr>
<tr><td colspan="2">Criterios:
Buenas prácticas en los controles de cambios: Solicitud de cambio- autenticación- aceptación- priorización- diseño de cambio- prueba de cambio- implementación- documentación.</td></tr>
<tr><td>Información requerida</td><td>Métodos de Análisis</td></tr>
<tr><td>Política y/o procedimientos de la gestión de cambios, diagrama de flujo de procesos

Estatuto del comité para el control de cambios

Documentación para el cambio: solicitud de cambio, procedimientos de pruebas de control de cambio, plan de aseguramiento de calidad, plan y procedimientos de pruebas

Informes y registros del software para la gestión del cambio

Actas de la reunión del consejo de control de cambios

Informes breves de gestión de cambio considerados por la gerencia</td><td>1. Verificar la existencia de procedimientos de gestión de cambios debidamente aprobados, asegurando que definan roles, flujos de trabajo y responsabilidades para controlar cualquier modificación en el entorno de TI; para ello, se revisan políticas de cambios, manuales operativos y actas de aprobación; como evidencia, buscar versiones vigentes de procedimientos, registros de difusión y actas de validación.
2. Verificar si se han establecido los procedimientos para la iniciación, revisión y aprobación de los cambios, así como la planificación de los tiempos y la asignación de responsabilidades para la ejecución de estas tareas.
3. Entrevista al personal, observar las prácticas reales y revisar los documentos para garantizar que se cumpla con los procedimientos de gestión del cambio: consulta para verificar el cambio, rastrear el cambio hasta el entorno operativo, verificar el cumplimiento de los procedimientos de solicitud, por ejemplo, revisión y priorización realizada por la gerencia, y verificar la existencia de la aprobación y la documentación.
4. 6. Verificar si el equipo de aseguramiento de la calidad (QA) de la Entidad ha realizado auditorías al proceso de gestión de cambios, y si el área de TI ha revisado los informes y registros asociados, asegurando que todos los cambios hayan sido documentados y registrados adecuadamente en el software de gestión de cambios
5. Garantizar que el acceso a la biblioteca fuente de producción (por ejemplo: código fuente,</td></tr>
</table>

	configuraciones) esté limitado al personal de CM, y que el área de TI evite cambios no autorizados en el entorno operativo. 6. 8. Revisar la documentación y prácticas vigentes para asegurar que los usuarios finales de la organización estén involucrados en las pruebas de los cambios, a fin de garantizar su validez y exactitud funcional. 7. Asegurar que cada cambio en los sistemas o recursos tecnológicos tengan un registro formal de aprobación y cierre por parte de las áreas pertinentes de la Entidad antes de su implementación en el entorno de producción.
Tema 5 de auditoría: Ejecución de cambios estándares ¿Los cambios en TI se realizan de forma planificada y se garantiza que la organización puede volver a una versión anterior si es necesario?	
Criterios: Buenas prácticas de gestión del cambio: se programan los cambios y se documentan los procedimientos y responsabilidades para la recuperación de áreas afectadas debido al impacto no deseado de los cambios.	
Información Requerida	**Métodos de Análisis**
Políticas y procedimientos de gestión de cambios aprobados. Documentación sobre pruebas e implementación de cambios Cronogramas de implementación y ventanas de mantenimiento. Registros de cambios de configuración y recuperación de documentación Copia de seguridad y procedimientos de	1. Verificar que todos los cambios propuestos hayan sido evaluados considerando su impacto técnico, operativo, de seguridad de la información y de cumplimiento normativo, y que hayan sido priorizados y aprobados en función de su importancia, impacto y urgencia; para ello, se revisan solicitudes de cambio (RFC), matrices de impacto y actas de comité de cambios; como evidencia, buscar registros de aprobación, matrices firmadas y priorizaciones documentadas. 2. Verificar que se realizaron pruebas antes de la implementación de los cambios en ambientes controlados, asegurando que se validará su correcto funcionamiento previo al paso a producción; para ello, se revisan planes de prueba, reportes de ejecución y bitácoras de resultados; como evidencia, buscar reportes de pruebas firmados, logs de ambiente de pruebas y actas de validación. 3. Verificar que exista análisis de compatibilidad con otros sistemas para evitar reversiones o conflictos posteriores, asegurando la interoperabilidad de los cambios; para

recuperación Solicitudes de cambio (RFC) y matrices de impacto técnico y normativo. Actas de comité de cambios (CAB) y registros de priorización. Planes de pruebas y reportes de ejecución en ambiente controlado. Análisis de compatibilidad y matrices de interoperabilidad. Planes de respaldo, procedimientos de rollback y cronogramas de contingencia del período revisado Registros de monitoreo post-cambio y reportes de resultados.	ello, se revisan documentos de análisis de impacto, reportes técnicos y actas de comité técnico; como evidencia, buscar matrices de compatibilidad, informes de validación y registros de revisión. 4. Verificar que se mantienen planes de respaldo antes del paso a producción y planes de reversión (rollback) para aplicar en caso de fallos durante la implementación de cambios; para ello, se revisan planes de contingencia, procedimientos de respaldo y reportes de simulación; como evidencia, buscar planes firmados, cronogramas de respaldo y registros de pruebas de rollback. 5. Comprobar que se realiza una implementación controlada de cambios, de forma estructurada y programada, preferiblemente fuera de horarios críticos para minimizar el impacto en la continuidad de sistemas y servicios; para ello, se revisan cronogramas de implementación, actas de planificación y reportes de ejecución; como evidencia, buscar registros de ventanas de mantenimiento, cronogramas firmados y reportes de finalización. 6. Verificar que existan mecanismos de monitoreo posteriores a la implementación de los cambios, para detectar oportunamente posibles incidentes y evaluar si se alcanzaron los resultados esperados; para ello, se revisan planes de seguimiento, registros de monitoreo y reportes de validación post-implementación; como evidencia, buscar logs de monitoreo, reportes de resultados y actas de revisión. 7. 7. Revisión de la documentación, entrevista a los usuarios de la Entidad para verificar si los impactos imprevistos de los cambios o mejoras en la funcionalidad han sido abordados como prioridad, conforme a los intereses de la Entidad.

Tema 6 de auditoría: Cambios de emergencia ¿Están controlados adecuadamente los cambios de emergencia cuando los procedimientos establecidos para definir, autorizar, probar y documentar los cambios no se puedan cumplir?	
Información Requerida	**Métodos de Análisis**
Procedimientos de control de cambios de emergencia Documentación de cambios de emergencia que se han realizado durante el período auditado Bitácoras de incidentes post pasos a producción y actas de cierre. Registros de cambios de emergencia, bitácoras de incidentes y actas de cierre.	1. Revisión de los procedimientos de gestión de cambios para determinar si contienen una sección específica y un conjunto de procedimientos para controlar cambios de emergencia en los sistemas e infraestructura tecnológica. 2. Verificar la documentación de cambios de emergencia realizados durante el período auditado, confirmando que incluyan análisis de resultados y validación posterior; para ello, se revisan registros de cambios de emergencia, bitácoras de incidentes y actas de revisión; como evidencia, buscar reportes firmados de cambios urgentes, registros de seguimiento y reportes de cierre. 3. Solicitar un ejemplo de cambio de emergencia. Comparación con un procedimiento documentado. Verificar qué pruebas se han realizado, previo a la introducción en el entorno de producción. En caso de no existir un procedimiento documentado, preguntar cómo saben qué hacer y quién aprueba tales cambios. 4. Examinar si los cambios de emergencia son aprobados por un Servidor Público autorizado según la política antes de pasar a producción.

Tema 7 de auditoría: Procedimientos post cambios ¿Se cumple con los procedimientos adecuados para la actualización de los sistemas y la documentación de usuario con posterioridad a la implementación de un cambio?	
Criterios: Buenas prácticas de gestión de cambio (por ejemplo, COBIT 5-BAI dominio, ITIL sobre Soporte del Servicio)	
Información Requerida	**Métodos de Análisis**
Documentación del proceso de funcionalidades afectadas por el cambio Procedimientos establecidos para la documentación	1. Verificar que las áreas responsables del cambio comunican a las otras unidades para garantizar la integridad, coherencia y actualización de los cambios implementados, ¿Se cumplieron con los procedimientos operativos, actualización de los elementos de configuración (CI), documentación de aplicaciones, pantallas de ayuda y materiales de capacitación con el mismo procedimiento de gestión de cambio y si estas actividades fueron consideradas como parte integral del cambio? 2. Verificar si existe un período adecuado de conservación para la documentación de los cambios, para el sistema de cambio previo y posterior, y para la documentación del usuario. 3. Verificar qué mecanismos existen para actualizar los procesos del negocio para cambios en el hardware o el software a fin de garantizar que se utiliza una funcionalidad nueva o mejorada.

3.3 Gestión de incidentes y problemas	
Objetivo de auditoría: Evaluar la eficacia de los procedimientos para la gestión de incidentes y problemas de la Entidad.	
Tema 8 de auditoría: Procedimiento de gestión a incidentes ¿Existe una política documentada de respuesta a incidentes y están los usuarios del negocio en conocimiento de ella?	
Criterios: Buenas prácticas en respuesta a incidentes.	
Información Requerida	**Métodos de Análisis**
Políticas y/o procedimientos de gestión de incidentes y problemas.	1. Verificar si existen políticas y/o procedimientos formales para la gestión de incidentes y problemas, y si estos documentos están aprobados, actualizados , si en ellos

Directrices para la comunicación con terceros externos en relación con los incidentes Registros de clasificación y priorización de incidentes y problemas. Matrices de impacto, urgencia y prioridad. Reportes de análisis técnico de incidentes recurrentes. Registros de escalamiento y actas de comité de problemas. Procedimientos de mesa de servicio y matrices de escalamiento. Acuerdos de Nivel de Servicio (SLA). Bitácoras de incidentes atendidos y reportes de cierre. Registros de análisis causa-raíz y actas de acciones correctivas. Registros de medidas disciplinarias, cambios aprobados o constancias de capacitación.	se define claramente la asignación de responsabilidades y se establecen los canales de atención y comunicación tanto para usuarios internos como externos. 2. Verificar que existan mecanismos documentados y operativos para la gestión de incidentes y problemas, confirmando que se cuente con lineamientos claros para la detección, registro, análisis, solución, cierre de cada caso, y post- incidente; para ello, se revisan políticas de gestión, manuales operativos y registros de incidentes; como evidencia, buscar procedimientos vigentes, bitácoras de atención y reportes de cierre. 3. Revisar la existencia y funcionamiento de los canales de atención para el reporte y seguimiento de incidentes, verificando el registro de los casos, tiempos de atención y respuesta de escalamiento y/o cierre. 4. Constatar la clasificación y priorización de incidentes y problemas, verificando que permitan determinar de forma objetiva el impacto, la urgencia y la prioridad para su resolución oportuna; para ello, se revisan registros de incidentes, matrices de clasificación y procedimientos operativos; como evidencia, buscar bitácoras de incidentes, matrices firmadas y reportes de priorización. 5. Revisión de los procedimientos reales mediante los cuales los usuarios del negocio tienen conocimiento de la política, y la naturaleza de la comunicación entre el equipo de respuesta a incidentes (mesa de ayuda) y las partes interesadas del negocio. 6. Entrevista con una muestra de usuarios del negocio en toda la organización para obtener una garantía sobre la concientización del plan de respuesta a incidentes.

<table>
<tr><td colspan="2">Tema 9 de auditoría: Conjunto de habilidades y recursos
¿Existe un equipo de respuesta a incidentes adecuadamente calificado que posea las herramientas adecuadas, los recursos y el respaldo de la dirección de TI para gestionar los incidentes?</td></tr>
<tr><td colspan="2">Criterios:
Buenas prácticas para la respuesta a incidentes, directrices NIST, como lo establece el SLA.</td></tr>
<tr><td>Información Requerida</td><td>Métodos de Análisis</td></tr>
<tr><td>Política y plan de respuesta a incidentes

Capacitación para la concientización de respuesta a incidentes, estrategia de actualización de las habilidades requeridas del personal de respuesta a incidentes (IRT)

Lista de herramientas de registro y aplicaciones utilizadas para el monitoreo y uso de la red</td><td>1. Verificar informes del análisis técnico aplicado para gestionar incidentes y problemas recurrentes, asegurando que, de ser necesario, se permita escalar a otras instancias de soporte o gestión; para ello, se revisan reportes de análisis, registros de incidentes escalados y actas de comité de problemas; como evidencia, buscar informes técnicos, registros de escalamiento y resultados de seguimiento.
2. Revisar los procedimientos de la mesa de servicio para verificar que se hayan definido e implementado mecanismos de escalamiento para incidentes que no puedan ser resueltos de forma inmediata, conforme lo definido en el Acuerdo de Nivel de Servicio (SLA); para ello, se revisan manuales de procedimientos, matrices de escalamiento y acuerdos de SLA; como evidencia, buscar procedimientos firmados, registros de escalamiento y bitácoras de seguimiento.</td></tr>
<tr><td colspan="2">Tema 10 de auditoría: Eficacia de la respuesta a incidentes operativos de TI
¿La estrategia de respuesta a incidentes resulta efectiva?</td></tr>
<tr><td colspan="2">Criterios:
Buenas prácticas de respuesta a incidentes (COBIT 5 dominio DSS, ITIL sobre Soportes de Servicio)</td></tr>
<tr><td>Información requerida</td><td>Métodos de Análisis</td></tr>
<tr><td>Medidas a tomar para la respuesta a incidentes, registros de formularios, etc.

SLA´s de atención, escalamientos y cierres

Procedimientos de manejo de incidentes: directrices para la priorización de incidentes</td><td>1. Verificar si se ha asignado a cada servicio una prioridad de respuesta o tratamiento de incidentes.
2. Verificar si se identificó la fuente del incidente y constatar las medidas adoptadas para corregir o mitigar su recurrencia, como procedimientos de cambio, medidas disciplinarias o acciones de capacitación al personal involucrado; para ello, se revisan registros de incidentes, reportes de análisis causa-raíz y actas de acciones correctivas; como evidencia, buscar reportes de causa-raíz, registros de cambios y constancias de capacitación o medidas</td></tr>
</table>

Informes de casos y medidas adoptadas	aplicadas. 3. Verificar si el equipo de respuesta a incidentes registra todos los incidentes resueltos en detalle y revisa la información por posibles actualizaciones de la base de conocimientos.

3.4 Gestión de Servicios	
Objetivo de auditoría: Evaluar si el área de TI monitorea activamente las operaciones de TI de conformidad con el Acuerdo de Nivel de Servicio interno o el contrato suscrito.	
Tema 11 de auditoría: Parámetros de servicios ¿Qué criterios básicos de medición de servicios están cubiertos por el SLA interno (OLA) entre la organización y el área de TI?	
Criterios: Buenas prácticas de SLA, asignación de responsabilidades entre los responsables de los procesos del negocio y el área de TI, objetivos documentados de la organización para la gestión de la red, ofertas de servicios y parámetros, definición por tipo de problemas, responsabilidades de la mesa de servicios.	
Información Requerida	**Métodos de Análisis**
Catálogo completo y actualizado de servicios TI. SLA interno de la entidad, entre el directorio o las otras áreas de la Entidad y el área de TI Responsabilidades en la atención del servicio Informes de servicio generados Usuario/tiempo de respuesta de la aplicación	1. Comprobar que se mantiene un listado o catálogo completo y actualizado de los servicios TI, asegurando que incluya la descripción, alcance y responsables de cada servicio ofrecido; para ello, se revisan catálogos de servicios, registros de actualización y actas de validación; como evidencia, buscar versiones vigentes del catálogo, bitácoras de cambios y registros de aprobación. 2. Revisión de los Acuerdos de Nivel de Servicio (SLA) definidos por el área de TI de la entidad, a fin de determinar si incluyen los elementos apropiados, como objetivos de nivel de servicio claros, detallados y mensurables; descripción de los sistemas y servicios cubiertos; parámetros de calidad del servicio (QoS); servicios excluidos o no cubiertos; alcance del soporte técnico y resolución de problemas a nivel de aplicación; niveles de disponibilidad del sistema; horarios de atención de la mesa de servicios; tiempos de respuesta y resolución según la clasificación de la gravedad de los problemas; parámetros de rendimiento; cronogramas de mantenimiento programado, y la identificación clara de quién provee, quién consume y quién supervisa cada

	servicio. Para ello, se deben revisar los SLA firmados, sus anexos técnicos y las matrices de responsabilidades; como evidencia, se recomienda recopilar copias de los SLA vigentes, cronogramas de monitoreo y actas de revisión periódica. 3. Verificar que se cuente con registros para la gestión de los servicios incluidos en el listado o catálogo, asegurando que exista trazabilidad de actividades, incidencias, solicitudes y mejoras implementadas; para ello, se revisan bitácoras de gestión, registros operativos y reportes de seguimiento; como evidencia, buscar historiales de tickets, reportes de atención y registros de mejoras.
Tema 12 de auditoría: Cumplimiento del Servicio ¿Qué mecanismos existen para garantizar que el SLA se cumpla sistemáticamente?	
Criterios: El área responsable por los servicios de TI, Implementación, monitoreo y modificación del SLA/OLA, de ser necesario, en base a la evolución de los servicios, niveles de demanda y requerimientos de usuarios; aplica medidas de corrección y reforzamiento para reducir los incumplimientos en el servicio.	
Información Requerida	**Métodos de Análisis**
Catálogo completo y actualizado de servicios TI. Parámetros del SLA Informes de plazos Diagramas o gráficos que muestran el éxito o fracaso de cómo se cumplen estos acuerdos a lo largo del tiempo Documentos de las reuniones periódicas que revisan el análisis de las bases de referencia y las tendencias Parámetros operacionales Sanciones y compensaciones relacionadas al servicio	1. Verificar si los responsables de los procesos de la Entidad han firmado el acuerdo de nivel de servicios (SLA/OLA). 2. Revisión de los informes que el área de TI genera diariamente o en cualquier otro intervalo de tiempo. Verificar si todos los indicadores acordados están siendo monitoreados por medio de informes/gráficos de tendencias, etc. 3. Revisión de los informes para examinar qué parámetros se miden y se reportan a la dirección periódicamente. 4. Revisión de los documentos para verificar que los informes de las actividades de la mesa de servicios sean considerados por la dirección y comparados con las solicitudes de resolución, y que los temas esenciales sean considerados para las decisiones de compra y para la revisión periódica del SLA/OLA. 5. Verificar que en el SLA/OLA se hayan establecido sanciones, compensaciones o planes de mejora para casos de incumplimiento, y que se haya evidenciado la aplicación de estos mecanismos cuando correspondía;

Bitácoras de gestión de servicios, registros operativos e históricos de tickets. Informes de cumplimiento de SLA, OLA (Operational Level Agreement) y UC (Underpinning Contracts). SLA firmados, anexos técnicos y matrices de responsabilidades. Contratos o acuerdos con cláusulas de sanciones y compensaciones. Reportes de incumplimientos y planes de mejora aplicados.	para ello, se revisan cláusulas contractuales, reportes de incumplimientos y actas de comité de seguimiento; como evidencia, buscar contratos con cláusulas específicas, reportes de aplicación de sanciones y registros de ejecución de planes de mejora. 6. Verificar qué medidas ha tomado la unidad de TI o, en caso de un grupo del soporte de TI subcontratado, por la dirección de la Entidad, si los parámetros operacionales no corresponden con los requerimientos del SLA/OLA.
Tema 13 de auditoría: Eficacia del Servicio ¿La gestión de servicios de TI garantiza la satisfacción de los usuarios y ayuda a cumplir los objetivos de la Entidad?	
Criterios: Consecución de los parámetros de desempeño que se ajustan a las necesidades y a los objetivos del negocio.	
Información Requerida	**Métodos de Análisis**
Informes de la mesa de servicios, actas de las reuniones entre las partes interesadas del negocio y el área de TI Temas de agenda para los ciclos de revisión del SLA/OLA Registros de tickets con fechas de inicio, atención, escalamientos y cierres. Registros de encuestas de	1. Verificar si la entidad cuenta con sistemas automatizados para el registro, seguimiento y control de las solicitudes de servicios; verificar si los sistemas implementados proveen facilidades de flujo automatizado de trabajo para el escalamiento y gestión de tickets. 2. Verificar que se realicen encuestas o reuniones con los usuarios finales para evaluar la satisfacción respecto a los niveles de servicio, y que se documenten resultados y planes de acción derivados; para ello, se revisan encuestas aplicadas, minutas de reuniones y reportes de resultados; como evidencia, buscar formularios de encuestas, actas de retroalimentación y reportes de análisis de satisfacción. 3. Verificar si el tiempo de resolución de problemas

satisfacción y reuniones con usuarios. Reportes de análisis de resultados y acciones de mejora derivadas. Cronogramas de revisión y actas de comité de servicio.	reportados fue inferior al de los parámetros establecidos en el SLA/OLA, para lo cual se puede seleccionar una muestra de solicitudes y calcular los tiempos para los hitos, luego determinando el porcentaje de cumplimiento; podría utilizar herramientas CAAT para procesar los registros provenientes del sistema de tickets del helpdesk. 4. Verificar que los SLA/OLA se revisen regularmente para ajustarse a las necesidades institucionales, considerando la evolución de los servicios, niveles de demanda y requerimientos de usuarios; para ello, se revisan cronogramas de revisión, actas de comités y registros de actualización; como evidencia, buscar actas firmadas, matrices comparativas de ajustes y versiones actualizadas de SLA/OLA.

3.5 Gestión de Activos de TI	
Objetivo de auditoría: Evaluar si el área de TI gestiona los activos de TI (ITAM), durante el ciclo de vida completo de todos los activos de TI de la organización, con el fin de maximizar su valor, controlar los costos, gestionar los riesgos y apoyar la toma de decisiones relacionadas con la compra, reutilización, retiro y disposición de los activos	
Tema 14 de auditoría: Parámetros clave ¿La organización gestiona el ciclo de vida de los activos de TI, considerando su alta, ubicación, custodio, mantenimiento y entre otros?	
Criterios: La organización debe tener formalizado los procesos para gestionar el ciclo de vida de los activos tecnológicos.	
Información Requerida	**Métodos de Análisis**
Registros de ciclo de vida de activos y manuales de gestión. Inventarios actualizados y listas de clasificación por tipo y criticidad. Etiquetas de identificación y reportes de control físico. Planes de mantenimiento, bitácoras de soporte y reportes	1. Verificar la documentación del detalle del ciclo de vida de los activos, confirmando que contemple fases de adquisición, uso, mantenimiento, renovación y disposición final; para ello, se revisan registros de gestión de activos, manuales de ciclo de vida y bitácoras de seguimiento; como evidencia, buscar cronogramas de gestión, registros de actualización y actas de baja de activos. 2. Verificar que los activos estén clasificados por tipo, nivel de criticidad o confidencialidad, y que cuenten con identificadores únicos o etiquetado que facilite su control, rastreo y protección; para ello, se revisan registros de inventario, políticas/procedimientos de clasificación y

de intervención. Actas de entrega-recepción y registros de custodia de activos. Informes de verificaciones periódicas y conciliaciones contables. Inventarios de licencias de software y reportes de estado. Contratos de adquisición, mantenimiento, soporte y garantías. Procedimientos de clasificación de activos o de bienes.	listas de activos; como evidencia, buscar inventarios actualizados, etiquetas de identificación y reportes de control físico. 3. Verificar reportes de mantenimiento y soporte a equipos de TI, asegurando que se realicen conforme a planes establecidos y se documenten adecuadamente las intervenciones; para ello, se revisan planes de mantenimiento, bitácoras de soporte y reportes de intervención; como evidencia, buscar reportes de mantenimiento firmados, actas de servicio y cronogramas de actividades. 4. Verificar que cada activo tenga un custodio designado formalmente, respaldado por actas de entrega-recepción o documentos equivalentes que definan responsabilidades; para ello, se revisan registros de asignación de custodios, actas de entrega y formularios de recepción; como evidencia, buscar actas firmadas, listas de responsables y registros de movimientos. 5. Constatar informes de verificaciones periódicas de activos, para asegurar que se mantengan actualizados su estado y ubicación, permitiendo la correcta actualización del inventario y su coherencia con el registro contable; para ello, se revisan reportes de verificaciones físicas, conciliaciones de inventario y registros contables; como evidencia, buscar informes firmados, actas de conciliación y registros contables alineados. 6. Verificar la gestión de licencias de software, confirmando la determinación del estado de las licencias (válidas o caducadas) e informes que detallen los riesgos identificados de carácter legal, de seguridad de la información u otros relacionados; para ello, se revisan inventarios de licencias, reportes de cumplimiento y análisis de riesgos asociados; como evidencia, buscar bases de datos de licencias, reportes de auditoría y planes de regularización. 7. Verificar el registro de contratos de adquisición, mantenimiento, soporte y garantías, asegurando que cumplan con las obligaciones legales y contractuales establecidas; para ello, se revisan contratos firmados, anexos legales y cronogramas de cumplimiento; como evidencia, buscar copias de contratos, registros de renovaciones y comprobantes de vigencia.

	8. Verificar las disposiciones que garanticen que los datos son eliminados de forma segura antes de la remoción o reutilización de equipos, validando que existan procedimientos y registros que respalden la eliminación; para ello, se revisan políticas de eliminación segura, bitácoras de borrado y certificados de destrucción; como evidencia, buscar procedimientos firmados, registros de borrado y actas de disposición final.

ANEXO 5. EXTERNALIZACIÓN

MATRIZ SUGERIDA PARA LA AUDITORÍA

4.1 Cumplimiento legal y normativo de externalización de servicios de TI	
Objetivo de auditoría: Evaluar si la entidad cuenta con una política adecuada para la externalización que esté alineada a las normativas de adquisición de servicios vigente.	
Tema 1 de auditoría: Elementos claves de la externalización de los servicios ¿Cuenta la organización con una política de externalización?	
Criterios: Política Organizacional sobre externalización y gestión de los contratos de servicios.	
Información Requerida	**Método(s) de Análisis**
Política de externalización de los servicios de TI y procedimientos relacionados Proceso de aprobación para la externalización de una función/servicio Lista de las funciones/servicios externalizados Lista de las funciones/servicios externalizados o con externalización parcial Modalidad de servicio por parte del proveedor de servicios Análisis de costos y beneficios de la externalización de una función/servicio Lista de proveedores de servicios externalizados con sus ubicaciones Documentos relativos a la aprobación de funciones/servicios externalizados	1. Verificar la existencia de política o procedimientos de externalización de servicios de TI, que esté actualizada, debidamente aprobada y alineada con los principios de gobernanza de TI y los objetivos estratégicos de la entidad; para ello, se revisan versiones de la política, actas de aprobación y documentos de alineación estratégica; como evidencia, buscar políticas vigentes, actas firmadas y referencias en planes estratégicos. 2. Revisar que la política o procedimiento de externalización haya sido difundida a las áreas involucradas, incluyendo TI, jurídico, adquisiciones y procesos usuarios de los servicios, garantizando conocimiento y aplicación; para ello, se revisan registros de difusión, correos de notificación y actas de reuniones de socialización; como evidencia, buscar constancias de difusión, listas de asistencia y circulares internas. 3. Revisar la política y/o procedimiento para verificar (por ejemplo) que contenga información sobre los activos de la organización que pueden o no ser externalizados y determine la lista de servicios/funciones que ésta puede externalizar. 4. Revisar los documentos para verificar que la organización haya identificado los riesgos conexos en relación con las diferentes modalidades de externalización, y la ubicación geográfica del proveedor de los servicios externalizados. 5. Revisar la documentación para verificar si la organización ha garantizado la continuidad del negocio, los derechos a los datos, seguridad, titularidad y costo estén incluidos en el contrato de servicios que cubre el caso de la adquisición, incluso ante la

Estrategia para garantizar la continuidad en el caso que otra organización asuma el control del proveedor de servicios Información sobre cualquier adquisición del proveedor de servicios Documentos/informes de seguimiento Política de adquisición o equivalente Lista de leyes que regulan la adquisición y externalización	terminación prevista o anticipada del servicio. 6. Revisar la documentación para evaluar que el procedimiento incluya la identificación de los parámetros de monitoreo para las funciones externalizadas y que requiera que éstos sean incluidos en el acuerdo de externalización. 7. Verificar que los contratos de bienes y servicios externalizados cumplieron con las cláusulas y normativa aplicable de contratación pública, protección de datos personales, confidencialidad y responsabilidad; para ello, se revisan contratos firmados, anexos legales y reportes de cumplimiento normativo; como evidencia, buscar contratos completos, revisiones legales y dictámenes de cumplimiento. 8. Verificar que los contratos y acuerdos de nivel de servicio (SLA) hayan sido suscritos formalmente por el representante legal o delegado de la entidad y el representante legal del proveedor, asegurando su validez legal; para ello, se revisan contratos originales, firmas legales y anexos; como evidencia, buscar copias firmadas, registros de aprobación y certificados de autenticidad. 9. Revisar el acuerdo de confidencialidad para verificar que toda la información relevante esté resguardada conforme a los términos pactados; para ello, se revisan cláusulas de confidencialidad, anexos legales y reportes de cumplimiento; como evidencia, buscar acuerdos firmados, validaciones legales y registros de auditoría de cumplimiento. 10. Verificar la existencia de un acuerdo sobre la propiedad de los datos y de las aplicaciones para el soporte de las operaciones, así como la devolución oportuna de estos al finalizar los servicios, incluyendo garantías de acceso y tiempo para la migración de servicios, aplicaciones y datos, y su posterior eliminación segura en plataformas del proveedor; para ello, se revisan contratos, cláusulas de propiedad intelectual y planes de migración; como evidencia, buscar contratos firmados, planes de devolución y certificados de eliminación.

<table>
<tr><td colspan="2">Tema 2 de auditoría: Monitoreo y supervisión del contrato de externalización de servicios
¿Existen mecanismos de monitoreo y seguimiento de los servicios provistos?, ¿Se toman las medidas adecuadas cuando no se cumplen las disposiciones del acuerdo de nivel de servicio?</td></tr>
<tr><td colspan="2">Criterios:
Disposiciones/parámetros definidos en el Acuerdo de Nivel de Servicio y las medidas de seguimiento de la organización.</td></tr>
<tr><td>Información Requerida</td><td>Método(s) de Análisis</td></tr>
<tr><td>Contrato/Acuerdo de Nivel de Servicio

Cronogramas aprobados, referencias, costos y otros parámetros técnicos que definen el producto o servicio adquirido o externalizado

Documentos/informes de seguimiento/actas de reuniones de las revisiones realizadas, medidas a tomar, indicaciones al proveedor (órdenes de trabajo, descripción de las tareas, etc.)

Análisis del impacto de las desviaciones detectadas, determinación de acciones a ejecutar e instrucciones específicas para el Contratista.

Informes de Acciones tomadas sobre las desviaciones de los niveles de servicio</td><td>1. Verificar la existencia de indicadores de desempeño y métricas de calidad, así como la descripción clara de los parámetros de medición del servicio; para ello, se revisan SLA, matrices de indicadores y reportes de cumplimiento; como evidencia, buscar indicadores definidos, resultados de medición y reportes de revisión.
2. Revisión de la documentación para evaluar si se han establecido cambios no autorizados en los acuerdos de nivel de servicio.
3. Revisar los informes y registros de monitoreo y seguimiento de los servicios prestados por el proveedor, validando que se evalúe el cumplimiento de lo establecido en el contrato y los SLA ; para ello, se revisan reportes de monitoreo, actas de comité de seguimiento y registros de validación; como evidencia, buscar informes periódicos, actas firmadas y reportes de resultados de SLA.
4. Revisión de los informes de seguimiento para identificar las deficiencias /desviación del servicio y evaluación del impacto debido a las mismas.
5. Revisión de las notificaciones e informes sobre las medidas tomadas para verificar que éstas se adecuen al impacto en las disposiciones del negocio y contractuales.
6. Verificar que el proveedor realice el monitoreo del servicio en la nube y que este monitoreo sea verificado periódicamente por la entidad para asegurar su calidad; para ello, se revisan reportes de monitoreo del proveedor, actas de revisión y registros de validación; como evidencia, buscar reportes firmados, registros de revisión y resultados de verificación.
7. Verificar que exista control de acceso a los servicios e información alojados en la nube, asegurando que se</td></tr>
</table>

	proteja la confidencialidad, integridad y disponibilidad de los datos; para ello, se revisan configuraciones de seguridad, matrices de permisos y pistas de auditoría; como evidencia, buscar políticas de acceso, bitácoras de actividad y reportes de seguridad.
Tema 3 de auditoría: Protección de datos y gestión de datos ¿Están los derechos de protección de datos y acceso incorporados al contrato de servicio? ¿Están los datos apropiadamente definidos como para cubrir los datos productivos, así como los programas/software que los procesan, según corresponda? ¿Existe un mecanismo para garantizar que el proveedor de servicios adopta e implementa los requerimientos en cuanto a la protección de datos y la seguridad, de conformidad con el Acuerdo de Nivel de Servicio?	
Criterios Los requerimientos respecto de los derechos de acceso y protección de datos de la organización, se comunican y son aplicados por la Contratista.	
Información Requerida	**Método(s) de Análisis**
Requerimientos respecto de los derechos de acceso y Protección de Datos de la Organización Definición de los datos (para protección y derechos de acceso) Contrato con el proveedor de servicios Lista de los registros de acceso de datos del proveedor de servicios Informes de auditorías de terceros o propias con recomendaciones y seguimiento de estas Informes del monitoreo Correspondencia con el proveedor de servicios sobre el tema Informes de gestión de incidentes Acuerdo de no divulgación con la entidad contratada	1. Revisión de la documentación sobre la adecuación de los requerimientos para la protección de datos y derechos de acceso/definición de datos. 2. Revisión de la documentación del contrato con el proveedor de servicios para verificar la incorporación de los requerimientos sobre protección de datos y derechos de acceso. 3. Verificar que los procesos, datos y software estén bajo control de la entidad, asegurando que no se pierda la administración ni el acceso a información crítica; para ello, se revisan contratos, procedimientos de control y registros de acceso; como evidencia, buscar cláusulas de control, bitácoras de acceso y validaciones de cumplimiento. 4. Verificar la existencia de acceso a los datos y redes alojados por el proveedor, especialmente al concluir el contrato, garantizando la continuidad y control de la información; para ello, se revisan cláusulas contractuales, procedimientos de acceso y registros de control; como evidencia, buscar contratos con cláusulas claras, bitácoras de acceso y registros de validación.

Lista de la información divulgada por la entidad contratada a terceros, parte(s) no vinculada(s)	5. Revisión de la documentación de los informes de auditoría de terceros/propias. 6. Revisión de la documentación de los informes de la supervisión, correspondencia e informes de gestión de incidentes para evaluar las actividades de seguimiento de la Entidad. 7. Revisión del acuerdo de confidencialidad para verificar que toda la información relevante sea cubierta. 8. Verificar si la divulgación de la información por parte de la entidad externalizada ha sido autorizada
Tema 4 de auditoría: Gestión de Proveedores en el Exterior ¿La Organización recibe servicios de proveedores extranjeros, o las subcontrataciones de estos procesan datos en servidores fuera del país?	
Criterios: Disposiciones de la política de externalización relacionadas con la externalización de entidades en el exterior. Leyes del país que regulan las actividades del negocio con entidades en el exterior.	
Información Requerida	**Método(s) de Análisis**
Lista de leyes y reglamentos relacionados con la externalización de servicios Información sobre cualquier presencia en el país del proveedor de servicios Lista de oficinas de la organización ubicadas en el exterior Lista de leyes y reglamentos que regulan al proveedor de servicios en su país Acuerdo bilateral entre el país de la organización y el país del proveedor de servicios que facilite acuerdos de externalización	1. Revisión de la documentación para evaluar que la organización haya identificado los riesgos relacionados con la externalización de proveedores de servicios en el exterior. 2. Revisión de la documentación para evaluar si el análisis del costo-beneficio abordó los riesgos relacionados con la externalización de proveedores de servicios en el exterior. 3. Revisión de la documentación para evaluar la existencia de un sistema sólido para garantizar el cumplimiento del Acuerdo de Nivel de Servicio y el contrato de externalización. 4. Revisión de la documentación para evaluar que el seguimiento de cualquier desviación del Acuerdo de Nivel de Servicio y del contrato se realiza oportunamente, garantizando un tiempo de inactividad y pérdida mínimo para la organización. Nota: Los Servicios realizados en el extranjero. En el caso que la entidad externalice servicios de procesamiento de datos fuera del país, debería disponer en todo momento de los

Informes sobre el desempeño anterior del proveedor en cuanto a plazos de entrega y cuestiones de calidad Reportes de monitoreo y seguimiento de SLA. Indicadores de desempeño y métricas de calidad. Análisis de costos y beneficios del proveedor de servicios local y del exterior Contrato de externalización y Acuerdo de Nivel de Servicio Información sobre el monto del depósito/garantía financiera relacionada con el desempeño Lista de las desviaciones al Acuerdo del Nivel de Servicio y el contrato de externalización Informes de monitoreo y seguimiento de las medidas adoptadas por el proveedor de servicio respecto de las desviaciones	antecedentes de la empresa contratada. En especial, deberá mantener aquellos antecedentes que respalden la solidez financiera del proveedor del servicio y que éste mantiene certificaciones de calidad, seguridad y apropiados sistemas de control.
Tema 5 de auditoría: Prácticas para mantener la titularidad del conocimiento y procesos del negocio. ¿Está bien delineada y documentada la titularidad de los procesos del negocio? ¿Se garantiza que no se producirá una pérdida de conocimiento del negocio debido a la externalización? ¿Existe capacidad para llevar a cabo internamente los servicios de externalización? ¿Se puede garantizar la continuidad del negocio si el proveedor no puede prestar los servicios en el futuro?	

Criterios:

Las Organizaciones mantienen el conocimiento del negocio y son capaces de continuar con sus operaciones internamente para la función esencial de la misión, si los contratistas o proveedores son incapaces de prestar el servicio. Conservar la titularidad de los procesos del negocio. Mantener el conocimiento de la Entidad. Desarrollo en relación con la continuidad del negocio ante la falta de prestación del servicio por parte del proveedor en cualquier momento.

Información Requerida	Método(s) de Análisis
Identificación de los procesos del negocio y habilidades esenciales que se deben mantener internamente. Documentación de los procesos de la Entidad. Documento detallado del diseño del sistema de servicios de externalización de la Entidad. Lista de capacitación del personal en los procesos de la Entidad, diseño de sistemas, datos, software de aplicación. Informes de incidentes/correspondencia relacionados con la interrupción del servicio/disputa con el proveedor de servicios, incluidas aquellas relacionadas con la titularidad del sistema /datos. Actas de las reuniones con el contratista. Planes y registros de evidencia de transferencia de conocimiento.	1. Revisión de la documentación para evaluar si la organización mantiene la titularidad de los procesos, datos y software de aplicación por medio de disposiciones adecuadas contenidas en el contrato. 2. Validar que el personal de la entidad reciba el traspaso de conocimientos de los bienes y/o servicios contratados durante la vigencia del contrato, garantizando la transferencia técnica necesaria; para ello, se revisan planes de transferencia, cronogramas de capacitación y registros de ejecución; como evidencia, buscar actas de capacitación, listas de asistencia y cronogramas firmados. 3. Verificar la existencia de acceso a los datos y redes alojados por el proveedor, especialmente al concluir el contrato, garantizando la continuidad y control de la información; para ello, se revisan cláusulas contractuales, procedimientos de acceso y registros de control; como evidencia, buscar contratos con cláusulas claras, bitácoras de acceso y registros de validación. 4. Revisión de la documentación para evaluar que el conocimiento de la Entidad en términos de datos, software de aplicación, diseño de sistemas esté bien documentado y que el personal se mantenga actualizado respecto de estos temas periódicamente a través de la capacitación, etc. 5. Revisión de la documentación para evaluar que la organización y su personal estén involucrados en las actualizaciones del sistema realizadas por la entidad subcontratada y que la documentación detallada sobre las actualizaciones al sistema sea proporcionada a la Entidad.
Tema 6 de auditoría: Acuerdo de Nivel de Servicio Externalizados ¿Está suficientemente detallado el acuerdo de nivel de servicio para identificar todas las funciones y responsabilidades entre la Entidad y el proveedor de servicios? ¿Se ha implementado con rigurosidad el acuerdo de nivel de servicio? ¿Cuenta la Entidad con un mecanismo para monitorear la implementación del acuerdo de	

nivel de servicio? ¿Existe un mecanismo disponible para abordar las excepciones al acuerdo de nivel de servicio?	
Criterios: El acuerdo de nivel de servicio es la base para el seguimiento y control del contratista o proveedor en relación con los requerimientos técnicos y de otro tipo.	
Información Requerida	**Método(s) de Análisis**
Acuerdos de nivel de servicio (SLA) o contratos firmados por ambas partes. Requerimientos técnicos y de otro tipo (lista de servicios a ser realizados por el proveedor) Lista de las responsabilidades de la Entidad y del proveedor Referencia para los servicios que se medirán, período de medición, duración, ubicación y cronogramas de presentación de informes (índices de defectos, tiempo de respuesta, horario del personal de atención al cliente, etc.). Informes periódicos del estado de desempeño de los proveedores SLA específicos para servicios en la nube con medidas de desempeño. Cláusulas y procedimientos de acceso a datos y redes en la nube. Reportes de monitoreo de servicios en la nube y registros de verificación.	1. Revisión de la documentación para evaluar que todos los requerimientos de los usuarios se traducen en requerimientos de nivel de servicios. 2. Revisión de la documentación para evaluar que las funciones y responsabilidades de la organización y del proveedor de servicio sean claramente identificadas y definidas. 3. Revisión de la documentación para evaluar que los parámetros para los niveles de desempeño sean claramente identificados e incluidos en el acuerdo de nivel de servicio. 4. Revisión de la documentación para evaluar que se ha establecido y acordado el mecanismo de monitoreo de nivel de servicio entre la organización y el proveedor de servicios. 5. Revisión de los informes de estado de los proveedores para evaluar que los parámetros en el SLA son informados por parte del contratista y revisados por personal pertinente dentro de la organización. 6. Evaluación del cumplimiento de los parámetros técnicos y referencias del SLA. 7. Verificación de las medidas adoptadas por la organización en relación con las desviaciones al acuerdo de nivel de servicio.

<table>
<tr><td colspan="2">Tema 7 de auditoría: Respuesta a los requerimientos de Seguridad
¿Ha identificado la Entidad los requisitos de seguridad con respecto a la externalización?
¿Existe un mecanismo que garantice que los requisitos de seguridad de la organización son abordados por el proveedor de servicios?
¿Cuenta la entidad con un mecanismo para monitorear el cumplimiento de los requisitos de seguridad por parte del proveedor de servicios?</td></tr>
<tr><td colspan="2">Criterios:
Los requisitos de seguridad pertinentes a la Entidad se aplican al contratista según corresponda.</td></tr>
<tr><td>Información Requerida

Política de seguridad de la organización.

Contrato de externalización.

Acuerdo del Nivel de Servicio.

Inventario de datos, hardware y software de aplicación con el proveedor de servicios.

Inventario de las copias de seguridad de archivos de datos y software de aplicación con el proveedor de servicios.

Registros de control de acceso de los archivos de datos, software de aplicación, así como hardware en la ubicación externalizada.

Plan de seguridad para el sitio de copia de seguridad y para el sitio de recuperación ante desastres.

Informes de seguimiento con respecto a problemas de seguridad.

Correspondencia entre la organización y el proveedor de servicios con respecto a las</td><td>Método(s) de Análisis

1. Revisión de la documentación para evaluar que los requerimientos de seguridad han sido identificados por la Entidad e incorporados al contrato de externalización o SLA.
2. Verificar si la Entidad cuenta con el inventario de los archivos de datos, software de aplicación. (Ver gestión de activos de información).
3. Verificar que la Entidad controle/ tenga conocimiento que el estado de los archivos de datos, software de aplicación y hardware se conserven durante el proceso de copia de seguridad y recuperación de datos llevado a cabo mediante externalización.
4. Verificar si la Entidad cuenta con la garantía de autorización de cualquier cambio en los datos, software de aplicación y hardware de la empresa subcontratada.
5. Verificar si la Entidad cuenta con una garantía en cuanto al acceso a los datos, aplicaciones de software y hardware en la ubicación subcontratada mediante un estudio de los registros de acceso (físico y lógico).
6. Verificar si la Entidad cuenta con la garantía de mecanismos de seguridad establecidos por el proveedor de servicios.
7. Verificar si la Entidad recibe regularmente informes y actas sobre la información en los reportes de monitoreo.</td></tr>
</table>

<table>
<tr><td>cuestiones de seguridad.</td><td></td></tr>
<tr><td colspan="2">Tema 8 de auditoría: Procedimientos para la copia de seguridad y recuperación.
¿Cumple el proveedor con los requerimientos del contrato o SLA para BCP y DRP?</td></tr>
<tr><td colspan="2">Criterios:
Acuerdo de nivel de servicio o contractual respecto del BCP y DRP con el proveedor.</td></tr>
<tr><td>Información Requerida

Contrato o SLA.

Auditoría Interna o certificación de terceros de la disponibilidad del BCP y DRP del proveedor.

Informes periódicos de las pruebas o actualizaciones del BCP/DRP.</td><td>Método(s) de Análisis

1. Revisar contratos o SLA para asegurar que el proveedor esté obligado a garantizar el BCP y DRP en los datos, aplicaciones y servicios externalizados.
2. Revisar contratos o SLA para asegurar que el proveedor proporcione los informes de auditoría interna o independiente que confirman que las actividades de BCP/DRP se han implementado y que el proveedor prueba sus procedimientos periódicamente.
3. Revisar los informes presentados por el proveedor para asegurar que las pruebas se hayan realizado de acuerdo con las condiciones del contrato y/o SLA.</td></tr>
</table>

ANEXO 6. GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO

MATRIZ SUGERIDA PARA LA AUDITORÍA

5.1 Política, plan y organización para la continuidad del negocio	
Objetivo de auditoría: Evaluar si existe una política y/o procedimientos efectivos de continuidad del negocio en la Entidad y recuperación ante desastres.	
Tema 1 de auditoría: Política y organización de la función para la continuidad del negocio ¿Cuenta la Entidad con un plan de contingencia y una política de continuidad del negocio, así como de recuperación ante desastres?	
Criterios: La Entidad cuenta con un plan de contingencia aprobado y adoptado, y una política que cubre de forma exhaustiva todas las áreas de operaciones de contingencia e identifica claramente los requerimientos de capacitación y cronogramas de prueba; y establece requerimientos en cuanto a roles y responsabilidades para los miembros del equipo	
Información Requerida	**Método(s) de Análisis**
Documento de Política de Continuidad del Negocio. Documento de Política de TI. Proceso de aprobación para el establecimiento de los objetivos de la política del negocio. Correspondencia y actas de las reuniones relacionadas con la continuidad del negocio. Organigrama del equipo de continuidad del negocio.	1. Verificar la existencia de una Política de Continuidad del Negocio, y que esta se encuentre aprobada, actualizada y comunicada suficientemente dentro de la Entidad. 2. Verificar que en la política o procedimientos para la continuidad del negocio se hayan definido los compromisos para asegurar la disponibilidad de los servicios críticos de TI ante interrupciones o fallos, detallando alcance, objetivos, roles, responsables y gestión de riesgos; para ello, se revisan políticas, procedimientos y actas de aprobación; como evidencia, buscar versiones vigentes, actas de validación y matrices de roles. 3. Revisar la documentación para evaluar que la política de Continuidad del Negocio sea coherente con las políticas generales de TI de la Entidad. 4. Verificar que la política o procedimiento de continuidad del negocio haya sido difundido de forma efectiva al personal y partes interesadas; para ello, se revisan registros de difusión, actas de reuniones y constancias de capacitación; como evidencia, buscar listas de asistencia, correos de notificación y circulares internas. 5. Revisar la documentación para evaluar que la política de Continuidad del Negocio aborda los requerimientos de continuidad del negocio mediante la definición de los objetivos de contingencia de la organización, el marco

	organizacional y las responsabilidades para la planificación de contingencias. 6. Revisar el contenido del plan de continuidad del negocio para determinar si incluyen aspectos a considerar antes, durante y posterior a la crisis. 7. Revisar la documentación para evaluar que los principales departamentos hayan designado miembros del equipo de recuperación ante desastres y que sus funciones sean claramente establecidas. 8. Verificar que el plan de continuidad del negocio incluya la planificación de contingencias, procedimientos para respuesta ante emergencias, recuperación de usuarios y actividades de gestión de crisis; para ello, se revisan anexos del BCP, procedimientos específicos y manuales de actuación; como evidencia, buscar diagramas de contingencia, protocolos de respuesta y cronogramas de crisis. 9. Evaluar que el plan de continuidad del negocio cubra todos los recursos de TI con la identificación clara de los sistemas y servicios críticos para la entidad; para ello, se revisan inventarios de activos críticos, matrices de impacto y anexos del BCP; como evidencia, buscar listas de activos críticos, registros de validación y matrices de priorización.
Tema 2 de auditoría: Continuidad basada en evaluación de riesgos ¿Se han llevado a cabo análisis de impacto del negocio y evaluaciones de riesgo, y se han identificado y priorizado datos críticos, software de aplicaciones, operaciones y recursos?	
Criterios: Marco de Gestión del Riesgo de la organización o equivalente. Política de Continuidad del Negocio o equivalente. Finalización de la evaluación del impacto del negocio e identificación de datos críticos, software de aplicación, operaciones y recursos.	

Información Requerida	Método(s) de Análisis
Informe(s) de Evaluación de Riesgo. Informe(s) de Evaluación del impacto del Negocio. Lista de datos críticos, software de aplicación, operaciones y recursos para cada función. Lista de riesgos residuales. Lista de interesados involucrados. Revisión de informe(s) sobre la evaluación de riesgo y el impacto en el negocio. Política/marco de la evaluación de riesgo de la organización. Actas de las reuniones sobre evaluación de riesgo y evaluación del impacto en el negocio.	1. Revisar la documentación para evaluar que se ha llevado a cabo la evaluación de riesgo, y que se han identificado las posibles amenazas y sus impactos de los sistemas y servicios críticos de la entidad 2. Revisar la documentación para evaluar que se han considerado todas las áreas funcionales en la evaluación de riesgo y la evaluación del impacto. 3. Revisar la documentación para evaluar que el análisis de impacto haya considerado el impacto provocado por cualquier interrupción en relación con el tiempo y otros recursos y sistemas conexos. 4. Revisar la documentación para evaluar que la decisión sobre los riesgos residuales se haya tomado en un nivel apropiado. 5. Revisar la documentación para evaluar que la organización haya determinado los RTO (objetivos de tiempos de recuperación) y RPO (Objetivos de puntos de recuperación) para cada aplicación crítica. 6. Revisar la documentación para evaluar que los RTO y RPO sean prácticos y razonables para cada aplicación y línea del negocio o función. 7. Verificar que el plan de continuidad del negocio (BCP) esté alineado con los requisitos de la Entidad y los riesgos identificados en el análisis de impacto al negocio (BIA); para ello, se revisan versiones del BCP, matrices de riesgos y reportes de análisis; como evidencia, buscar BCP aprobado, matrices de alineación y actas de revisión.
Tema 3 de auditoría: Planes de Recuperación ante Desastres. ¿el Plan de Continuidad del Negocio incluye planes de recuperación y copias de seguridad para los sistemas operativos, datos, software de aplicación y centro de procesamiento de datos (recuperación) y si han sido implementados adecuadamente?	
Criterios: Se determine la criticidad de las aplicaciones y funciones de conformidad con la Evaluación de Impacto del Negocio de la organización. Se determine la periodicidad de las copias de seguridad. Se documenten los planes de recuperación y copia de seguridad.	

Información Requerida	Método(s) de Análisis
Políticas y procedimientos de continuidad del negocio aprobados. Plan de continuidad del negocio (BCP) alineado a requisitos y riesgos. Planificación de contingencias, protocolos de respuesta y gestión de crisis. Inventarios de activos críticos y matrices de impacto. Procedimientos de evaluación y recuperación por sistema o aplicativo. Reportes de BIA y matrices de amenazas y riesgos. Plan de recuperación ante desastres (DRP) con anexos operativos. Evidencias de comunicación del DRP a personal clave. Políticas y procedimientos de respaldo y restauración. Roles y responsabilidades definidos para respaldo, restauración y contingencia. Registros de seguridad de respaldos, cifrado y control de acceso. Planes de contingencia con	1. Verificar que el plan de recuperación ante desastres (DRP) cuente con la descripción de actividades de la infraestructura que soportan los servicios de TI, incluyendo procedimientos para restaurar sistemas, datos y servicios tecnológicos, estrategias de recuperación, roles y responsabilidades; para ello, se revisan planes DRP, manuales operativos y anexos de roles; como evidencia, buscar DRP vigente, diagramas de restauración y actas de aprobación. 2. Verificar que el plan de recuperación ante desastres haya sido comunicado al personal de áreas técnicas y funcionales, garantizando su conocimiento; para ello, se revisan registros de capacitación, actas de difusión y constancias de participación; como evidencia, buscar listas de asistentes, actas de reunión y evidencias de divulgación. 3. Verificar que para el plan de respaldo y restauración se hayan definido políticas, procedimientos y herramientas para realizar copias de seguridad de datos, configuraciones y sistemas, considerando su criticidad, y su restauración conforme a los requisitos de tolerancia establecidos en el BCP; para ello, se revisan políticas de respaldo, manuales técnicos y registros de ejecución; como evidencia, buscar cronogramas de respaldos, logs de restauración y reportes de pruebas. 4. Verificar que los planes de respaldo se correspondan en su estrategia con los RPO declarados en el BIA. 5. Verificar que en el plan de respaldo y restauración se hayan definido roles y responsabilidades claras para su aplicación y seguimiento; para ello, se revisan matrices de roles, actas de comité y registros operativos; como evidencia, buscar matrices firmadas, diagramas de responsabilidad y actas de validación. 6. Verificar que en el plan de respaldo y restauración se hayan definido y aplicado procedimientos de seguridad de respaldos, incluyendo mecanismos de cifrado y control de acceso; para ello, se revisan políticas de seguridad, configuraciones técnicas y registros de control; como evidencia, buscar registros de cifrado aplicado, logs de acceso a respaldos y reportes de cumplimiento.

análisis de riesgos, sitios alternos, contratos externos y medidas de redundancia.	7. Revisar la documentación para evaluar si los procedimientos de copia de seguridad cuentan con detalles e instrucciones precisas para su ejecución. 8. Revisar la documentación para evaluar que el plan de recuperación ante desastres incluya los activos de información considerados esenciales. 9. Verificar que la seguridad, lógica o física, sea la adecuada para la ubicación de las copias de seguridad. 10. Revisión de la documentación para evaluar que el procedimiento detallado de recuperación haya sido diseñado e incluya un reajuste de los parámetros del sistema, instalación de parches, establecimiento de los ajustes de configuración, disponibilidad de la documentación del sistema y procedimientos operativos, reinstalación de la aplicación y del software del sistema, disponibilidad de la copia de seguridad más reciente y prueba del sistema.
Tema 4 de auditoría: Pruebas de Continuidad de Negocio y Recuperación ante Desastres ¿Ha examinado la Entidad sus procedimientos de BC y DR, y qué cambios (si los hubo) se han efectuado como resultado de la prueba?	
Criterios: La Entidad debe examinar sus procedimientos documentados de BCP y DRP a través de ejercicios o maquetas para garantizar que operan en condiciones reales. El personal involucrado en garantizar la continuidad debe tener el conocimiento de sus roles.	
Información Requerida	**Método(s) de Análisis**
Políticas y procedimientos de continuidad del negocio. Plan de continuidad del negocio. Cronograma de Plan de pruebas. Inventarios de activos críticos. Registros de ejecución, pruebas y validaciones de continuidad. Lista de criterios de prueba	1. Revisar que las pruebas al BCP y DRP se encuentren planificadas para su realización con la periodicidad establecida en las políticas respectivas. 2. Revisión de la documentación para determinar si todos los elementos necesarios para su realización están cubiertos para la prueba. 3. Revisión de la documentación para determinar si las pruebas se llevan a cabo oportunamente en los intervalos planificados. 4. Revisar los resultados de las pruebas del plan de continuidad y las acciones correctivas derivadas, asegurando la mejora continua; para ello, se revisan reportes de pruebas, bitácoras de simulacros y actas de comités de seguimiento; como evidencia, buscar resultados de simulacros, registros de fallas y planes de corrección. 5. Revisión de la documentación para determinar que las

como RTO y RPO, etc. Resultados de pruebas de continuidad y planes de acción correctiva. Procedimientos de evaluación y recuperación por sistema o aplicativo. Plan de recuperación ante desastres (DRP) con anexos operativos. Evidencias de comunicación del DRP a personal clave. Políticas y procedimientos de respaldo y restauración. Roles y responsabilidades definidos para respaldo, restauración y contingencia. Registros de seguridad de respaldos, cifrado y control de acceso. Resultado de la prueba y medidas adoptadas o recomendaciones de la prueba. Medidas de seguimiento para los resultados de la prueba.	pruebas hayan sido llevadas a cabo en relación con los criterios identificados. 6. Revisión de la documentación para determinar que las recomendaciones hayan sido transmitidas a las autoridades correspondientes para su seguimiento. 7. Revisión de la documentación para determinar que las recomendaciones de las pruebas hayan sido debidamente cumplidas y el plan de continuidad del negocio o el plan de recuperación ante desastres hayan sido adecuadamente actualizados.

MATRIZ SUGERIDA PARA LA AUDITORÍA

6.1 Evaluación de Riesgos de Seguridad de la Información	
Objetivo de auditoría: Garantizar que todos los riesgos relativos a la seguridad de la información hayan sido Identificados, e implementado una estrategia adecuada de mitigación.	
Tema 1 de auditoría: Mecanismo de evaluación de riesgos de seguridad de la información. ¿Cuenta la Entidad con un eficaz y bien documentado mecanismo de evaluación de riesgos respecto a la seguridad de la información?	
Criterios: La política interna, los procedimientos o regulaciones muestran la disposición de la organización para enfrentar los riesgos críticos.	
Información Requerida	**Método(s) de Análisis**
Política de Riesgos de la Entidad Política de Riesgos de TI Política de Seguridad de SI. Procedimientos formales para la gestión de riesgo. Documento de Evaluación de Riesgos de la Seguridad de la Información Plan de Gestión de Riesgos de Seguridad de la Información (*aka, Plan de tratamiento de riesgos*) Matriz de Riesgos y Controles	1. Verificar que la política de gestión de riesgo de la Entidad haya considerado los requerimientos de evaluaciones de riesgos de seguridad de la información en el contexto de los riesgos de TI. 2. Verificar la existencia de un marco o metodología para el proceso de las evaluaciones de riesgos de la seguridad la información[1], aprobado y actualizado. 3. Verificar que se haya realizado la evaluación de riesgos de la seguridad, y este se encuentre aprobado, comunicado, actualizado, y elaborado conforme al marco adoptado. 4. Verificar que el proceso de evaluación de riesgos de seguridad de la información incluya el contexto del ambiente, alcance, criterios de evaluación, criterios de impacto y de aceptación del riesgo; la Entidad y responsabilidades en el proceso de gestión del riesgo, etc. 5. Verificar que el proceso de evaluación de riesgos de seguridad de la información detalle el análisis para la identificación de riesgos inherentes, a través de la identificación de activos prioritarios, amenazas, controles existentes, consecuencias, estimación del riesgo, metodología, y una valoración de las consecuencias (ej. criticidad, frecuencia, probabilidad e impacto). 6. Verificar que el proceso de evaluación de riesgos de seguridad de la información detalle la evaluación del riesgo, en la cual se realiza la comparación de los riesgos estimados con los criterios de evaluación, en función de las propiedades de la seguridad de la información: Confidencialidad, Integridad, Disponibilidad, Autenticidad (CIDA). 7. Verificar que el proceso de evaluación de riesgos de

	seguridad de la información detalle el tratamiento del riesgo, a partir de los resultados obtenidos del análisis y la evaluación del riesgo, así como los controles necesarios para mitigar el riesgo a niveles aceptables; por ejemplo, seleccionando los controles específicos que deberán ser implementados sugeridos por la norma ISO/IEC 27002 o el EGSI. 8. Verificar que el proceso de evaluación de riesgos de seguridad de la información detalle, en los casos de que se deba aceptar el riesgo, la clara identificación de los riesgos asumidos por la organización; estos riesgos residuales, y la motivación de por qué no serán tratados o si serán tratados parcialmente deberán estar documentados. 9. Verificar que el proceso de evaluación de riesgos de seguridad de la información tenga como resultado un Plan de Gestión de Riesgos de Seguridad de la Información (*aka, plan de tratamiento de los riesgos*). 10. Verificar que el proceso evaluación de riesgos de seguridad de la información considere la comunicación del riesgo, para todas las áreas operacionales y sus responsables. 11. El proceso evaluación de riesgos de seguridad de la información, deberá contar con mecanismos de seguimiento y análisis crítico, que observe periódicamente los resultados, efectividad de los controles y análisis crítico para el mejoramiento continuo del proceso de gestión del riesgo. 12. En caso de ausencia de procedimientos formales y de documentos sobre evaluación de riesgo, no desestimar controles que se encuentran incorporados a los procedimientos operativos de la organización, verificar si el mecanismo de control compensatorio que se encuentra incorporado a las operaciones es eficaz.
[1] ISO 27005 gestión de riesgo de seguridad de la información, ISACA Marco de Riesgo de TI, COSO Marco de Gestión de Riesgos de la Organización.	

6.2 Política de Seguridad de la Información	
Objetivo de auditoría: Evaluar si existe orientación estratégica y respaldo adecuados respecto a la seguridad de la información en términos de una política de seguridad, su cobertura, la concientización y su cumplimiento por parte de toda la Entidad.	
Tema 2 de auditoría: Política de Seguridad de la Información ¿Cuenta la Entidad con una Política de Seguridad de la Información? ¿Está correctamente implementada y documentada? ¿Conforma un plan de seguridad de TI coherente y sólido?	
Criterios: La política de seguridad de la información de la organización cubre todos los riesgos operativos y es capaz de proteger razonablemente los activos de información importantes del negocio contra pérdida, daño o abuso.[53]	
Información Requerida	**Método(s) de Análisis**
Estrategia de TI Política de seguridad de la información. Actas de aprobación y matrices de alineación con objetivos estratégicos. Textos de la política con referencias a leyes, reglamentos y estándares aplicables. Políticas de privacidad y protección de datos personales. Modelos de formularios o mecanismos empleados para el consentimiento informado y registros de aceptación. Logs de tratamiento de datos personales y reportes de control.	1. Verificar si el documento de la estrategia de TI destaca adecuadamente el papel fundamental de la seguridad de la información. 2. Verificar la existencia de una Política de Seguridad de la Información, aprobada, actualizada y comunicada a toda la organización. 3. Verificar que la política de seguridad de la información esté alineada con los objetivos estratégicos de la organización y con el Esquema Gubernamental de Seguridad de la Información (EGSI) u otra normativa vigente en el ámbito de seguridad, garantizando coherencia con estándares nacionales e internacionales; para ello, se revisan versiones de la política, planes estratégicos y matrices de alineación; como evidencia, buscar políticas vigentes, actas de comité y registros de validación. 4. Verificar que la política de seguridad de la información haga referencia explícita a leyes, reglamentos y estándares que la institución debe cumplir, tales como protección de datos personales, ciberseguridad y contratos; para ello, se revisan textos completos de la política, anexos legales y referencias normativas; como evidencia, buscar versiones firmadas, matrices de cumplimiento legal y dictámenes jurídicos. 5. Verificar la existencia de lineamientos claros que aseguren la privacidad y el consentimiento informado en el tratamiento de datos personales, conforme a la normativa aplicable; para ello, se revisan cláusulas de privacidad, políticas de protección de datos y registros de consentimiento; como evidencia, buscar políticas específicas de datos personales, formularios o Pantallas de

Plan de seguridad de TI con roles, responsabilidades y cronogramas de actividades. Registros de capacitaciones y evidencias de programas de concientización. Actas de comité de seguridad de la información.	consentimiento. 6. Verificar que la política contemple las consideraciones para la protección de la privacidad y el consentimiento en el tratamiento de datos personales. 7. Verificar que exista un plan de seguridad de TI en el que se definan claramente roles y responsabilidades, así como acciones de concientización y capacitación de los usuarios en seguridad de la información; para ello, se revisan planes de seguridad, cronogramas de capacitación y actas de comité; como evidencia, buscar versiones del plan, registros de roles asignados y listas de asistencia a capacitaciones. 8. Consultar y utilizar la matriz de *Gobernanza de TI* para *la estrategia de TI; a*nte la falta de una estrategia de TI por escrito, entrevistar a la máxima autoridad, a la dirección de nivel intermedio y al personal para verificar cuál es su conocimiento sobre el papel estratégico de la seguridad de la información. 9. Comparar los objetivos de la política y los procedimientos de seguridad para determinar la efectividad de la incorporación de los requerimientos de seguridad de la información en el plan de seguridad de TI
Tema 3 de auditoría: Contenido de la Política de Seguridad de la Información ¿Cuenta la organización con una política conforme lo establece la EGSI y/o 27002?	
Criterios: La política de seguridad de la información de la organización debería contener los aspectos mínimos indicados en la EGSI o 27002.	
Información Requerida	**Método(s) de Análisis**
Política de seguridad de la información. Políticas temas específicos Documentos esenciales (EGSI)	1. Verificar que se cuente con la **documentación esencial** establecida en el Esquema Gubernamental de Seguridad de la Información (EGSI), aprobadas por la dirección, publicadas, comunicadas y reconocidas por personal y las partes interesadas pertinentes, y revisadas a intervalos planificados si se producen cambios significativos, a saber: a) Proceso de gestión de riesgos de Seguridad de la información b) Informes de evaluación y de gestión de riesgos c) Plan de gestión de riesgos d) Política de Seguridad de la información a partir de los riesgos y amenazas identificados en la gestión de riesgos; que incluya el alcance de Implementación del Sistema de Gestión de la Seguridad de la Información (SGSI), definiciones, los Objetivos de

	Seguridad de la Información, principios guía de todas actividades relacionadas con seguridad de la información, compromiso con los requisitos y la mejora continua del SGSI, las responsabilidades (acordes a EGSI), procedimientos para tratar las extensiones (lo no contemplado en estas) y las excepciones. e) Políticas específicas por temas relevantes, según sea necesario para ordenar aplicación de controles de seguridad de la información. f) Declaración de aplicabilidad (este podría ser considerado el plan de implementación de la seguridad, que contiene todos los controles implementados o no, y las justificaciones de exclusión, o las compensaciones. g) Procedimiento de respuesta a incidentes de seguridad de la información h) Registros de las capacitaciones, habilidades, experiencia y cualificaciones i) Reportes, seguimiento y mediciones de los indicadores asociados a la seguridad de la información, ciberseguridad, privacidad de datos y continuidad del negocio. j) Programa o plan de auditoría interna al sistema de gestión de seguridad de la información y/o a sus componentes. k) Resultados de las Auditoría Internas realizadas al SGSI. l) Resultado de las revisiones por parte de la dirección o de las autoridades al SGSI. m) Registros de las actividades de usuarios que impactan en la seguridad (accesos, incidentes, infracciones, etc.) n) Inventario de activos de información (datos e información, arquitectura, servicios, software, hardware, redes y telecomunicaciones, instalaciones, personal clave, etc.) o) Uso aceptable de los activos de información por personal y proveedores p) Matriz de Requisitos reglamentarios y contractuales. q) Procedimientos Operativos de Seguridad para la Gestión de TI (vinculados con el componente de Operaciones) r) Política de control de accesos s) Definición de configuraciones de seguridad (deberían

	estar también incluidas en la CMDB de gestión de la configuración) t) Principios de ingeniería de sistemas seguros. 2. Revisar que la política de seguridad de la información y las políticas específicas por tema se encuentren aprobadas por la alta dirección, estén publicadas, comunicadas y reconocidas por el personal y partes interesadas pertinentes, revisadas a intervalos planificados y actualizadas si se producen cambios significativos; para ello, se revisan versiones vigentes, actas de aprobación, evidencias de publicación y registros de difusión; como evidencia, buscar políticas firmadas, circulares internas, constancias de capacitación y registros de revisiones periódicas. 3. Verificar que la política de seguridad de la información considere requisitos derivados de la estrategia y necesidades de la entidad, así como de normativa aplicable, legislación vigente, contratos y acuerdos relevantes, y contemple los riesgos y amenazas actuales y proyectadas de seguridad de la información; para ello, se revisan documentos de alineación estratégica, matrices de cumplimiento legal y análisis de riesgos; como evidencia, buscar matrices de vinculación, reportes de riesgos y referencias a contratos o normativas aplicables. 4. Comprobar que la política de seguridad de la información contenga declaraciones claras sobre la definición de seguridad de la información, objetivos o marco para establecer objetivos, principios rectores para todas las actividades relacionadas con seguridad, compromiso de satisfacer requisitos aplicables, compromiso de mejora continua del SGSI, asignación de responsabilidades a funciones definidas y procedimientos para la gestión de extensiones y excepciones; para ello, se revisan textos completos de la política, anexos explicativos y procedimientos vinculados; como evidencia, buscar versiones aprobadas de la política, desgloses temáticos y registros de aprobaciones de procedimientos complementarios. 5. Verificar que cualquier cambio en la política de seguridad de la información haya sido aprobado por la alta dirección, validando que exista registro formal de revisiones y actualizaciones; para ello, se revisan actas de comité, resoluciones administrativas y versiones históricas; como evidencia, buscar actas firmadas de revisión, cronologías de

	versiones y registros de control de cambios. 6. Confirmar que la política de seguridad de la información esté respaldada por políticas específicas por temas, como control de accesos, uso de redes, cifrado, gestión de incidentes, continuidad y otras necesarias, para ordenar la aplicación de controles de seguridad de la información de forma coherente; para ello, se revisan políticas complementarias, manuales operativos y lineamientos específicos; como evidencia, buscar políticas temáticas firmadas, manuales de aplicación y registros de capacitación o divulgación.

53 véase la serie ISO 27000 sobre el Sistema de Gestión de Seguridad de la Información y otras políticas internas, procedimientos o regulaciones aplicables.

6.3 Organización de la Seguridad de TI	
Objetivo de auditoría: Garantizar la operación segura de las instalaciones de procesamiento de TI.	
Tema 4 de auditoría: Estructura y responsabilidad para las actividades de seguridad de TI 1. ¿Cuenta la entidad auditada con una clara estructura de seguridad de TI? 2. ¿Están definidos los roles y las responsabilidades relativas a la seguridad con respecto a la política de seguridad de la información? 3. Validar que los contratos y acciones de personal de los funcionarios incluyan cláusulas sobre deberes y responsabilidades en seguridad de la información. 4. Revisar la existencia de procedimientos para la incorporación de requisitos de seguridad en el desarrollo de software o adquisición de sistemas, infraestructura de TI y servicios.	
Criterios: Roles y responsabilidades de TI claros y documentados referidos a la Política de Seguridad de la Información[54]	
Información Requerida	**Método(s) de Análisis**
Organigrama de la Entidad Organigrama de TI Organigrama de Seguridad de TI Regulaciones internas relativas a la seguridad de SI. Descripciones de las tareas Actas de reuniones de	1. Verificar que la máxima autoridad haya designado al interior de la Institución, un Comité de Seguridad de la Información (CSI), que estará integrado por los responsables de las siguientes áreas o quienes haga sus veces: Planificación quien lo presidirá, Talento Humano, Administrativa, Comunicación Social, Tecnologías de la Información, Jurídica y el delegado de protección de datos. 2. Verificar que las designaciones de los roles y funciones del comité de seguridad de la información hayan sido comunicadas formalmente a los responsables designados, asegurando que conozcan sus deberes y compromisos; para ello, se revisan actas de designación, comunicaciones internas y registros de aceptación; como evidencia, buscar

los órganos pertinentes. Actas de designación de roles y funciones del comité de seguridad. Comunicaciones internas de notificación de responsabilidades. Constancias de acuse de recibo y registros de aceptación. Agendas y actas de reuniones de coordinación entre unidades y áreas de TI. Minutas de seguimiento y matrices de acuerdos alcanzados. Contratos de trabajo y acciones de personal con cláusulas de seguridad. Anexos legales sobre deberes y confidencialidad. Manuales de funciones y políticas de seguridad aplicables. Procedimientos para requisitos de seguridad en desarrollo, adquisición e infraestructura.	actas firmadas, correos de notificación y constancias de acuse de recibo. 3. Verificar que la máxima autoridad haya designado al interior de su Institución a un funcionario como Oficial de Seguridad de la Información (OSI); y comunicado formalmente al responsable designado, asegurando que este conozca sus deberes y compromisos; para ello, se revisan actas de designación, comunicaciones internas y registros de aceptación; como evidencia, buscar actas firmadas, correos de notificación y constancias de acuse de recibo. 4. Verificar que el Comité de Seguridad de la Información (CSI) esté en funcionamiento, se haya reunido, a lo menos, ordinariamente de forma bimestral; y se haya informado semestralmente a la máxima autoridad los avances de la implementación del EGSI. 5. Verificar que el Oficial de Seguridad de la Información (OSI) se encuentra en funciones; que los roles, responsabilidades, y el perfil definido en el manual de cargos y funciones o equivalente de la entidad esté conforme a lo establecido en el EGSI.
Tema 5 de auditoría: Coordinación de las actividades de seguridad de TI ¿De qué manera la Entidad coordina las actividades de seguridad de la información entre sus diferentes áreas ?	
Criterios: Inexistencia de conflictos de responsabilidad, discordancia, vacíos de responsabilidad en las actividades de Seguridad de la Información.[55]	

Información Requerida	Método(s) de Análisis
Requerimientos legales respecto a la información clasificada. Estructura de la organización. Regulaciones Internas relativas a la seguridad de SI. Actas de la reunión del comité de seguridad de TI. Informes de fallas.	1. Verificar la existencia de documentación de reuniones de coordinación entre las unidades involucradas y las áreas de TI, comprobando que los temas tratados y acuerdos alcanzados consten en actas debidamente formalizadas; para ello, se revisan agendas de reuniones, actas de coordinación y listas de acuerdos; como evidencia, buscar actas firmadas, minutas de seguimiento y matrices de acuerdos. 2. Verificar los documentos, observar las prácticas y entrevistar al personal para determinar si hay conflictos/ superposiciones/ disparidades inherentes entre los procedimientos de seguridad que cumplen los empleados en diferentes departamentos/ unidades. 3. Verificar los procedimientos del flujo de trabajo operativo para identificar si cierta información es transmitida a terceros fuera del control de las unidades/empleados responsables.

54 véase Serie ISO 27000.

55 véase Serie ISO 27000 sobre Sistema de Gestión de Seguridad de la Información.

6.4 Gestión de Activos de Información	
Objetivo de auditoría: Fomentar la adecuada protección de los activos de TI.	
Tema 6 de auditoría: Gestión de Activos ¿Cuenta la Entidad con un sistema de gestión de activos adecuado, que respalde la seguridad de la información?	
Criterios: Garantizar la adecuada protección de los activos de información [58]	
Información Requerida	**Método(s) de Análisis**
Política de gestión de activos. Clasificación de Activos. Clasificación de información. Procedimientos de disposición de activos Informes de auditoría financiera (si se refieren	1. Verificar la existencia de un inventario actualizado de activos de información, incluyendo hardware, software, datos y servicios, con identificación clara y custodio asignado para cada activo; para ello, se revisan registros de inventario, bases de datos patrimoniales y actas de asignación; como evidencia, buscar inventarios actualizados, fichas de activos y registros de custodia firmados. 2. Verificar que los inventarios de activos de TI se encuentren documentados y actualizados, identificando su

a activos e inventarios). Inventarios actualizados de activos (hardware, software, datos, servicios). Bases de datos patrimoniales y fichas de activos (bienes nacionales) con custodios asignados. Bitácoras de mantenimiento y registros de procedencia y estado. Matrices de clasificación de activos y políticas de gestión. Políticas de uso de equipos, Internet y dispositivos móviles. Registros de socialización y capacitación del personal. Procedimientos de control para teletrabajo y dispositivos móviles. Inventarios de licencias de software y contratos de adquisición. Bitácoras de ingreso/salida de activos y formularios de autorización.	procedencia, actividades de mantenimiento y estado de funcionamiento; para ello, se revisan reportes de inventario, bitácoras de mantenimiento y actas de revisión; como evidencia, buscar registros actualizados, cronogramas de mantenimiento y reportes de estado operativo. 3. Verificar la existencia de la clasificación de activos, considerando criterios de criticidad, confidencialidad, integridad y disponibilidad, para facilitar su protección adecuada; para ello, se revisan matrices de clasificación, políticas de activos y registros de revisión; como evidencia, buscar matrices aprobadas, listados de activos clasificados y actas de validación. 4. Revisar la existencia y difusión de políticas de uso aceptado y razonable de activos, tales como uso de equipos, acceso a Internet y uso de dispositivos móviles, verificando que hayan sido comunicadas al personal; para ello, se revisan textos de políticas, registros de socialización y actas de capacitación; como evidencia, buscar políticas vigentes, listas de asistencia y constancias de recepción. 5. Verificar la existencia y funcionamiento de controles implementados para la protección de activos utilizados fuera del entorno de la entidad, como en teletrabajo o mediante dispositivos móviles; para ello, se revisan procedimientos de seguridad, configuraciones de control y bitácoras de monitoreo; como evidencia, buscar registros de control de acceso remoto, reportes de seguimiento y evidencias de aplicación de medidas de protección. 6. Verificar que la entidad disponga de software instalado debidamente licenciado, asegurando la legalidad y cumplimiento de contratos; para ello, se revisan inventarios de licencias, contratos de adquisición y reportes de auditoría de software; como evidencia, buscar bases de datos de licencias, facturas de compra y reportes de revisión de cumplimiento. 7. Revisar bitácoras o registros de ingreso y salida de activos como laptops o dispositivos externos, para validar la trazabilidad y la autorización de los movimientos realizados; para ello, se revisan registros de control de activos, formularios de ingreso/salida y actas de autorización; como evidencia, buscar registros firmados, bitácoras actualizadas y autorizaciones de movimiento. 8. Revisar los procedimientos para la disposición de activos y el nivel de supervisión obligatoria, verificando que exista un

Procedimientos de disposición y registros de eliminación de datos. Actas de asignación de custodios y cronogramas de actualización de registros.	requerimiento de autorización para cualquier disposición o reutilización de equipos y que se garantice la eliminación de datos antes de la remoción o reutilización; para ello, se revisan políticas de disposición, bitácoras de baja y procedimientos de borrado seguro; como evidencia, buscar registros de autorización, certificados de eliminación de datos y actas de disposición final. 9. Verificar si se han implementado políticas de seguridad de la información de conformidad con la clasificación de sensibilidad (etiquetado) de los datos de la organización (por ejemplo, confidencial, sensible).
58 Serie ISO 2700 Sistema de Gestión de Seguridad de la Información, COBIT, y otras políticas, procedimientos y regulaciones internos aplicados).	

6.5 Seguridad física y del entorno	
Objetivo de auditoría: Prevenir el robo o daño de la infraestructura de TI, el acceso no autorizado, y la copia o visualización de información sensible.	
Tema 7 de auditoría: Seguridad de las instalaciones ¿Están asegurados los edificios y las áreas exteriores de la organización contra riesgos físicos y ambientales?	
Criterios: Asegurar que la seguridad física y ambiental cumple con los requerimientos de seguridad y clasificación de acuerdo con la sensibilidad de los activos de TI.	
Información Requerida	**Método(s) de Análisis**
Diagrama de red. Plan de Seguridad de las instalaciones. Informe periódico de las pruebas físicas. Informes de los servicios pertinentes (Ejemplo, departamento de Bomberos).	1. Verificar la existencia de políticas o procedimientos de seguridad física y del entorno, asegurando que estén aprobados y alineados con los estándares de protección de activos críticos; para ello, se revisan textos de políticas, manuales operativos y actas de aprobación; como evidencia, buscar versiones vigentes, actas firmadas y registros de divulgación. 2. Verificar que dichas políticas o procedimientos contemplen actividades específicas para control de acceso físico, protección ambiental y resguardo de instalaciones críticas como centros de procesamiento de datos (CPD's) o data centers; para ello, se revisan anexos de políticas, diagramas de control y manuales de operación; como evidencia, buscar matrices de control de acceso, planos de instalaciones y registros de validación. 3. Comprobar la existencia de controles físicos como

	cerraduras, cámaras de vigilancia, alarmas, detectores de humo, extintores, sistemas contra incendios, UPS, generadores y sistemas de respaldo energético, verificando que estén operativos y mantenidos; para ello, se realizan inspecciones físicas, se revisan registros de mantenimiento y bitácoras de verificación; como evidencia, buscar reportes de inspección, contratos de mantenimiento y fotografías de instalaciones. 4. Verificar la existencia y mantenimiento de sistemas de climatización y control ambiental (HVAC), incluyendo aires acondicionados en salas de servidores, control de humedad y temperatura, y sistemas de detección y extinción de incendios; para ello, se revisan contratos de mantenimiento, bitácoras técnicas y reportes de inspección; como evidencia, buscar registros de mantenimiento preventivo, reportes de pruebas y actas de validación técnica. 5. Revisión de la ubicación, diseño y de las medidas de precaución físicas para los elementos clave de la infraestructura tecnológica, por ejemplo; salas de servidores alineadas con pasillo frio/caliente, separadores de paredes ignifugo, etc.). 6. Verificar qué controles ambientales se han implementado (extintores, alarmas, sistemas de energía, perímetros, etc.), y las bitácoras de mantenimiento de estos elementos se encuentran vigentes. 7. Revisar la existencia de un Plan de Evacuación y Respuesta ante Emergencias, garantizando que esté aprobado, socializado y actualizado; para ello, se revisan versiones del plan, diagramas de rutas y actas de validación; como evidencia, buscar planos de evacuación, registros de capacitación y actas de simulacros. 8. Verificar que se hayan realizado simulacros y capacitaciones al personal sobre procedimientos de evacuación y respuesta ante emergencias; para ello, se revisan cronogramas de simulacros, listas de participantes y reportes de resultados; como evidencia, buscar actas de simulacros, registros fotográficos y constancias de asistencia. 9. Confirmar que las copias de seguridad se almacenan en ubicaciones físicas seguras, con controles de acceso y condiciones ambientales adecuadas para su protección; para ello, se revisan procedimientos de respaldo, bitácoras

	de almacenamiento y registros de seguridad; como evidencia, buscar registros de ubicación, controles de acceso físico y reportes de inspección ambiental. 10. Revisar que existan logs de acceso físico a instalaciones críticas y reportes de incidentes relacionados con la seguridad física, garantizando la trazabilidad de ingresos y salidas; para ello, se revisan bitácoras de ingreso, registros de control de visitas y reportes de seguridad; como evidencia, buscar logs firmados, reportes de eventos y bitácoras de incidentes. 11. Verificar que se realicen análisis posteriores a incidentes de seguridad física, como robo, accesos no autorizados o daños a instalaciones, documentando causas, impactos y medidas correctivas; para ello, se revisan reportes de incidentes, actas de investigación y planes de acción; como evidencia, buscar informes de incidentes, registros de medidas correctivas y actas de comité de seguridad. 12. Verificar para sistemas de misión crítica que se han implementado medidas de redundancia en los recursos de soporte ambiental y energético, y que provean alta disponibilidad.
Tema 8 de auditoría: Acceso físico a las instalaciones ¿De qué manera garantiza la Entidad que solo el personal autorizado tenga acceso a las instalaciones?	
Criterios: La organización implementa medidas de seguridad a fin de prevenir el acceso físico no autorizado a instalaciones clave de TI (sala de servidores, almacenamiento de datos, etc.)	
Información Requerida	**Método(s) de Análisis**
Plan de instalación del hardware de TI. Plan de Seguridad del sitio. Configuración de dispositivos. Informe periódico de pruebas físicas. Informes de incidentes. Políticas y procedimientos	1. Determinar qué medios son utilizados. Implementar las políticas y procedimientos relativos a la seguridad de las instalaciones (puertas, credenciales, molinetes, guardias, barreras, clave de acceso y acceso mediante lector de tarjeta, etc.) y determinar si dichos procedimientos constituyen una identificación y autenticación adecuadas. 2. Verificar que existan mecanismos de control progresivos y proporcionales para el acceso a las áreas sensibles de sus instalaciones, por ejemplo, carnet, pin pad, RFID, biometría, y la combinación de doble factor de ser requeridos. 3. Verificar posibles situaciones de riesgo al observar alto tráfico de entrada/salida, próximo a áreas sensibles. 4. Verificar quién mantiene y controla las asignaciones de control de acceso en las ubicaciones sensibles. Verificar si el

de seguridad física y ambiental aprobados. Anexos con actividades de control de acceso, protección ambiental y resguardo de CPD's. Planos de instalaciones críticas y diagramas de control físico. Contratos de mantenimiento de sistemas de seguridad física y ambiental. Reportes de inspección de cerraduras, cámaras, alarmas y sistemas de detección/extinción. Plan de Evacuación y Respuesta ante Emergencias actualizado. Actas de simulacros, listas de asistencia y registros de capacitación. Procedimientos de almacenamiento de copias de seguridad y controles de acceso. Bitácoras de acceso físico y reportes de incidentes. Informes de análisis posterior a incidentes, planes de acción y actas de seguimiento.	nivel de gestión es suficiente para la Seguridad de la Información. 5. Verificar si el acceso a las áreas seguras/salas seguras/ubicaciones de servidor se encuentra restringido. 6. Seleccionar una muestra de usuarios/empleados y determinar si su acceso a las instalaciones es apropiado en base a las responsabilidades de su trabajo. 7. Verificar si éstos informan los incidentes a un sistema de gestión de incidentes/ problemas. Verificar si estos se analizan y si las lecciones se han aprendido. 8. Revisar la existencia de un Plan de Evacuación y Respuesta ante Emergencias. 9. Confirmar que las copias de seguridad se almacenan en ubicaciones seguras y que éstas tengan controles de acceso y ambientales adecuados.

Tema 9 de auditoría: Protección contra Intrusiones ¿Cuenta y cumple la Entidad con una política de detección de intrusiones?	
Criterios: Procedimientos para prevenir intrusiones según se establece en la Política de Seguridad interna de la Entidad	
Información Requerida	**Método(s) de Análisis**
Plan de Seguridad del sitio. Configuración de dispositivos. Informes de incidentes.	1. Examinar de qué manera la unidad de seguridad de la Entidad toma conocimiento de que se ha producido una intrusión, a fin de proteger las ubicaciones. 2. Revisión de las instrucciones para conocer el Proceso de gestión de una intrusión a un espacio o edificio seguro. 3. Revisión de los informes de incidentes para identificar si la intrusión fue detectada a tiempo. 4. Verificar si la Entidad cuenta con una política clara de escritorio o pantalla limpios para evitar el acceso no autorizado.

6.5 Seguridad física y del entorno
Objetivo de auditoría: Prevenir el robo o daño de la infraestructura de TI, el acceso no autorizado, y la copia o visualización de información sensible.
Tema 7 de auditoría: Seguridad de las instalaciones ¿Están asegurados los edificios y las áreas exteriores de la organización contra riesgos físicos y ambientales?
Criterios: Asegurar que la seguridad física y ambiental cumple con los requerimientos de seguridad y clasificación de acuerdo con la sensibilidad de los activos de TI.

Información Requerida	Método(s) de Análisis
Diagrama de red. Plan de Seguridad de las instalaciones. Informe periódico de las pruebas físicas. Informes de los servicios pertinentes (Ejemplo, departamento de Bomberos).	1. Verificar la existencia de políticas o procedimientos de seguridad física y del entorno, asegurando que estén aprobados y alineados con los estándares de protección de activos críticos; para ello, se revisan textos de políticas, manuales operativos y actas de aprobación; como evidencia, buscar versiones vigentes, actas firmadas y registros de divulgación. 2. Verificar que dichas políticas o procedimientos contemplen actividades específicas para control de acceso físico, protección ambiental y resguardo de instalaciones críticas como centros de procesamiento de datos (CPD's) o data centers; para ello, se revisan anexos de políticas, diagramas de control y manuales de operación; como evidencia, buscar matrices de control de acceso, planos de instalaciones y registros de validación. 3. Comprobar la existencia de controles físicos como cerraduras, cámaras de vigilancia, alarmas, detectores de humo, extintores, sistemas contra incendios, UPS, generadores y sistemas de respaldo energético, verificando que estén operativos y mantenidos; para ello, se realizan inspecciones físicas, se revisan registros de mantenimiento y bitácoras de verificación; como evidencia, buscar reportes de inspección, contratos de mantenimiento y fotografías de instalaciones. 4. Verificar la existencia y mantenimiento de sistemas de climatización y control ambiental (HVAC), incluyendo aires acondicionados en salas de servidores, control de humedad y temperatura, y sistemas de detección y extinción de incendios; para ello, se revisan contratos de mantenimiento, bitácoras técnicas y reportes de inspección; como evidencia, buscar registros de mantenimiento preventivo, reportes de pruebas y actas de validación técnica. 5. Revisión de la ubicación, diseño y de las medidas de precaución físicas para los elementos clave de la infraestructura tecnológica, por ejemplo; salas de servidores alineadas con pasillo frio/caliente, separadores de paredes ignifugo, etc.). 6. Verificar qué controles ambientales se han implementado (extintores, alarmas, sistemas de energía, perímetros, etc.), y las bitácoras de mantenimiento de estos elementos se

	encuentran vigentes. 7. Revisar la existencia de un Plan de Evacuación y Respuesta ante Emergencias, garantizando que esté aprobado, socializado y actualizado; para ello, se revisan versiones del plan, diagramas de rutas y actas de validación; como evidencia, buscar planos de evacuación, registros de capacitación y actas de simulacros. 8. Verificar que se hayan realizado simulacros y capacitaciones al personal sobre procedimientos de evacuación y respuesta ante emergencias; para ello, se revisan cronogramas de simulacros, listas de participantes y reportes de resultados; como evidencia, buscar actas de simulacros, registros fotográficos y constancias de asistencia. 9. Confirmar que las copias de seguridad se almacenan en ubicaciones físicas seguras, con controles de acceso y condiciones ambientales adecuadas para su protección; para ello, se revisan procedimientos de respaldo, bitácoras de almacenamiento y registros de seguridad; como evidencia, buscar registros de ubicación, controles de acceso físico y reportes de inspección ambiental. 10. Revisar que existan logs de acceso físico a instalaciones críticas y reportes de incidentes relacionados con la seguridad física, garantizando la trazabilidad de ingresos y salidas; para ello, se revisan bitácoras de ingreso, registros de control de visitas y reportes de seguridad; como evidencia, buscar logs firmados, reportes de eventos y bitácoras de incidentes. 11. Verificar que se realicen análisis posteriores a incidentes de seguridad física, como robo, accesos no autorizados o daños a instalaciones, documentando causas, impactos y medidas correctivas; para ello, se revisan reportes de incidentes, actas de investigación y planes de acción; como evidencia, buscar informes de incidentes, registros de medidas correctivas y actas de comité de seguridad. 12. Verificar para sistemas de misión crítica que se han implementado medidas de redundancia en los recursos de soporte ambiental y energético, y que provean alta disponibilidad.

Tema 8 de auditoría: Acceso físico a las instalaciones ¿De qué manera garantiza la Entidad que solo el personal autorizado tenga acceso a las instalaciones?	
Criterios: La Entidad implementa medidas de seguridad a fin de prevenir el acceso físico no autorizado a instalaciones clave de TI (sala de servidores, almacenamiento de datos, etc.)	
Información Requerida	**Método(s) de Análisis**
Plan de instalación del hardware de TI. Plan de Seguridad del sitio. Configuración de dispositivos. Informe periódico de pruebas físicas. Informes de incidentes. Políticas y procedimientos de seguridad física y ambiental aprobados. Anexos con actividades de control de acceso, protección ambiental y resguardo de CPD's. Planos de instalaciones críticas y diagramas de control físico. Contratos de mantenimiento de sistemas de seguridad física y ambiental. Reportes de inspección de cerraduras, cámaras, alarmas y sistemas de detección/extinción.	1. Determinar qué medios son utilizados. Implementar las políticas y procedimientos relativos a la seguridad de las instalaciones (puertas, credenciales, molinetes, guardias, barreras, clave de acceso y acceso mediante lector de tarjeta, etc.) y determinar si dichos procedimientos constituyen una identificación y autenticación adecuadas. 2. Verificar que existan mecanismos de control progresivos y proporcionales para el acceso a las áreas sensibles de sus instalaciones, por ejemplo, carnet, pin pad, RFID, biometría, y la combinación de doble factor de ser requeridos. 3. Verificar posibles situaciones de riesgo al observar alto tráfico de entrada/salida, próximo a áreas sensibles. 4. Verificar quién mantiene y controla las asignaciones de control de acceso en las ubicaciones sensibles. Verificar si el nivel de gestión es suficiente para la Seguridad de la Información. 5. Verificar si el acceso a las áreas seguras/salas seguras/ubicaciones de servidor se encuentra restringido. 6. Seleccionar una muestra de usuarios/empleados y determinar si su acceso a las instalaciones es apropiado en base a las responsabilidades de su trabajo. 7. Verificar si éstos informan los incidentes a un sistema de gestión de incidentes/ problemas. Verificar si estos se analizan y si las lecciones se han aprendido. 8. Revisar la existencia de un Plan de Evacuación y Respuesta ante Emergencias. 9. Confirmar que las copias de seguridad se almacenan en ubicaciones seguras y que éstas tengan controles de acceso y ambientales adecuados.

Plan de Evacuación y Respuesta ante Emergencias actualizado. Actas de simulacros, listas de asistencia y registros de capacitación. Procedimientos de almacenamiento de copias de seguridad y controles de acceso. Bitácoras de acceso físico y reportes de incidentes. Informes de análisis posterior a incidentes, planes de acción y actas de seguimiento.	
Tema 9 de auditoría: Protección contra Intrusiones ¿Cuenta y cumple la Entidad con una política de detección de intrusiones?	
Criterios: Procedimientos para prevenir intrusiones según se establece en la Política de Seguridad interna de la Entidad	
Información Requerida	**Método(s) de Análisis**
Plan de Seguridad del sitio. Configuración de dispositivos. Informes de incidentes.	1. Examinar de qué manera la unidad de seguridad de la Entidad toma conocimiento de que se ha producido una intrusión, a fin de proteger las ubicaciones. 2. Revisión de las instrucciones para conocer el Proceso de gestión de una intrusión a un espacio o edificio seguro. 3. Revisión de los informes de incidentes para identificar si la intrusión fue detectada a tiempo. 4. Verificar si la Entidad cuenta con una política clara de escritorio o pantalla limpios para evitar el acceso no autorizado.

6.7 Gestión de incidentes y acontecimientos relacionados con seguridad TI	
Objetivo de auditoría: Evaluar la eficacia de los procedimientos para la gestión de incidentes de la Entidad cuanto a la seguridad de la información.	
Tema 12 de auditoría: Gestión de incidentes de seguridad ¿Se cuenta con un equipo para responder a los incidentes de seguridad de la información?	
Criterios: RedTeam, BlueTeam en Seguridad de la Información de la Entidad.	
Información Requerida	**Método(s) de Análisis**
Manuales y procedimientos de respuesta a incidentes aprobados. Bitácoras de incidentes y reportes históricos de casos gestionados. Matrices de impacto, urgencia y priorización de incidentes. Configuraciones de monitoreo automatizado y registros de alertas. Actas de designación del equipo de respuesta a incidentes. Matrices de roles y responsabilidades asignadas. Informes de cierre de incidentes con acciones de mejora implementadas. Planes de acción correctiva y actas de comité de seguridad. Procedimientos de reporte de incidentes y formularios	1. Comprobar si la Entidad responde adecuadamente a incidentes de seguridad de TI, asegurando que se apliquen procedimientos formales para su detección, análisis, contención, erradicación y recuperación; para ello, se revisan manuales de respuesta, registros de incidentes y actas de comité de seguridad; como evidencia, buscar procedimientos aprobados, bitácoras de respuesta y reportes de cierre. 2. Evaluar la trazabilidad y seguimiento de incidentes históricos, verificando que se mantengan registros completos de cada fase de gestión, desde su identificación hasta su resolución; para ello, se revisan bitácoras de incidentes, reportes históricos y registros de acciones correctivas; como evidencia, buscar logs firmados, cronologías de incidentes y actas de lecciones aprendidas. 3. Validar que los incidentes se gestionen considerando su impacto y urgencia, aplicando criterios de priorización y escalamiento definidos; para ello, se revisan matrices de clasificación, reportes de atención y registros de escalamiento; como evidencia, buscar matrices aprobadas, registros de priorización y bitácoras de seguimiento. 4. Verificar la existencia de monitoreo automatizado de seguridad para detectar incidentes de forma proactiva y oportuna, mediante sistemas de alertas, correlación de eventos y generación de reportes; para ello, se revisan configuraciones de sistemas de monitoreo, logs generados y reportes de eventos; como evidencia, buscar registros de alertas, reportes de correlación y bitácoras de validación técnica. 5. Comprobar que exista un equipo definido y formalmente asignado para atender incidentes de seguridad de TI, con roles y responsabilidades claros; para ello, se revisan matrices de roles, actas de designación y manuales de

de registro. Logs de correlación de eventos y bitácoras de validación.	operación del equipo de respuesta; como evidencia, buscar listas de responsables, actas firmadas y registros de actividades. 6. Comprobar que la gestión de incidentes genere acciones de mejora, documentando medidas preventivas y correctivas para reducir la probabilidad de recurrencia; para ello, se revisan reportes de incidentes, planes de acción y actas de comité de seguridad; como evidencia, buscar informes de lecciones aprendidas, cronogramas de acciones correctivas y registros de implementación. 7. Verificar que existan mecanismos claros y formales para el reporte de incidentes por parte de usuarios o áreas técnicas, garantizando su atención oportuna; para ello, se revisan procedimientos de reporte, canales habilitados y registros de reportes recibidos; como evidencia, buscar manuales de procedimiento, formularios de reporte y bitácoras de recepción de incidentes
6.8 Seguridad de la información ligada al personal	
Objetivo de auditoría: Garantizar que todos los empleados (incluidos los contratistas y todo usuario de datos sensibles) estén calificados para manejar datos y comprendan sus funciones y responsabilidades en cuanto a la seguridad de la información.	
Tema 13 de auditoría: Concientización y Capacitación ¿Es la capacitación un procedimiento efectivo para mejorar las habilidades profesionales del personal en materia de Seguridad de la Información?	
Criterios: Realización, alcance y frecuencia de la Capacitación en Seguridad de la Información de la Entidad.	
Información Requerida	**Método(s) de Análisis[59]**
Cronograma de capacitación. Resultados de las pruebas finales. Evaluación de la eficacia de la capacitación.	1. Verificar que la entidad haya establecido programas de concientización, educación y formación en materia de seguridad de la información 2. Verificar que la entidad ha realizado la concientización, educación y formación en materia de seguridad de forma periódica al personal. 3. Verificar que la entidad asegura la comprensión de las actividades de sensibilización, educación o formación evaluando las mismas al final de las actividades. 4. Verificar que la entidad, a través de las áreas especializadas, identifican, preparan y poner en práctica un plan de formación adecuado para los equipos técnicos cuyas funciones requieren conjuntos de habilidades y conocimientos específicos para gestionar la seguridad de la información.

	5. Verificar que se han formalizado en las políticas de la entidad, las medidas disciplinarias para violaciones a la seguridad de la Información.

[59] Recursos humanos con respecto a la Seguridad de la Información es uno de los temas clave en otras secciones como *Gobernanza* de *TI,* y posiciones de esta Matriz de Auditoría, como *Política de Seguridad de la Información* (concientización, responsabilidad, flujo de información de arriba hacia abajo, sanciones) o *Control de Acceso* (derechos de usuarios individuales).

MATRIZ SUGERIDA PARA LA AUDITORIA

7.1 Controles de datos de entrada	
Objetivo de auditoría: Evaluar si los datos válidos son ingresados en la aplicación por el personal autorizado.	
Tema 1 de auditoría: Validación de Entrada ¿Cuenta la aplicación con controles de validación de entrada adecuados?	
Criterios: Numerosas buenas prácticas constituyen la base de los criterios para los controles de validación de entrada, por ejemplo, que las reglas de validación sean exhaustivas, estén documentadas e implementadas en las interfaces de entrada de la aplicación; se documenten diferentes métodos e interfaces para el ingreso de datos; los datos inválidos son debidamente rechazados por la aplicación; los criterios de validación se actualizan de manera oportuna, adecuada y por medio de autorización; existen controles compensatorios, como registros y reglas de autorización ante la posibilidad de anular los controles de entrada; y existen controles y documentación adecuados para las interfaces de la aplicación.	
Información Requerida	**Método(s) de Análisis**
Requerimiento y reglas del negocio Tipos de entrada de datos Requerimientos de cumplimiento legales y externos Estructura de interfaces de datos con otras aplicaciones Diagramas de flujo del sistema Manuales de usuario y guías de operación del sistema. Reglas de validación Especificaciones de diseño de validaciones automáticas. Resultados de pruebas	1. Verificar si las reglas de validación fueron adecuadamente diseñadas y documentadas, solicitando a los dueños de los procesos que indiquen qué reglas de validación deben estar garantizadas en el proceso que se está evaluando, y si determinando si las reglas y requerimientos del negocio declaradas se encuentran en la documentación de la aplicación. 2. Solicitar una descripción funcional para cada tipo de entrada e información de diseño sobre el ingreso de registros. Revisar la funcionalidad y el diseño para corroborar la existencia de controles oportunos y completos, y de mensajes de error. 3. Verificar que existan validaciones automáticas para campos obligatorios, formatos y rangos de valores antes de su ingreso al sistema, asegurando que los datos sean consistentes y cumplan criterios de integridad definidos; para ello, se revisan especificaciones de diseño, manuales de usuario y reportes de pruebas funcionales; como evidencia, observar a los usuarios de las aplicaciones en sus verdaderas actividades; buscar capturas de pantalla de validaciones y de registros de configuración de las reglas de validación, ejecutar la aplicación en un entorno de testing y probar las diferentes interfaces para el ingreso de datos y analizar los registros de datos almacenados en la base de datos mediante el uso de CAAT. 4. Evaluar la existencia de controles que prevengan la

funcionales y casos de prueba ejecutados. Reglas de base de datos y diagramas entidad-relación. Registros de auditoría de datos duplicados y reportes de incidencias. Matrices de roles y permisos de usuarios. Bitácoras de control de acceso y logs de actividad. Configuraciones de auditoría y logs de cambios.	duplicación de registros o datos clave, confirmando que el sistema aplique restricciones o alertas para evitar inconsistencias; para ello, se revisan reglas de base de datos, diagramas de entidad-relación y reportes de incidencias; como evidencia, buscar definiciones de llaves primarias, reportes de auditoría de datos duplicados y registros de pruebas de control. 5. Evaluar la existencia de controles que prevengan la duplicación de registros o datos clave, confirmando que el sistema aplique restricciones o alertas para evitar inconsistencias; para ello, se revisan reglas de base de datos, diagramas de entidad-relación y reportes de incidencias; como evidencia, buscar definiciones de llaves primarias, reportes de auditoría de datos duplicados y registros de pruebas de control. 6. Verificar si las modificaciones a los datos ingresados quedan registradas en bitácoras o logs, asegurando la trazabilidad de los cambios realizados; para ello, se revisan configuraciones de auditoría del sistema, registros de logs y reportes de cambios; como evidencia, buscar logs de transacciones, reportes de actividad de usuarios y registros de revisión. 7. Evaluar si los criterios y los parámetros de validación de los datos ingresados coinciden con las regulaciones del negocio y obligan al rechazo de tipos de entrada dispares. En el caso de los sistemas de procesamiento *on-line*, verificar que los datos inválidos sean rechazados o editados al momento del ingreso y probar los controles lógicos/ controles de cálculos efectuados. 8. Consultar y controlar la documentación a fin de verificar la posibilidad de anular las validaciones del control de datos de entrada y los controles. Verificar si las acciones de anulación están debidamente registradas y revisadas para constatar su adecuación. Verificar si la autoridad para anular se limita solo al personal de supervisión y a un número restringido de situaciones. Examinar correcciones de errores, anulaciones de entrada y otros documentos para verificar que se cumplen los procedimientos. 9. Determinar qué interfaces existen en la aplicación. Estas interfaces podrían presentarse bajo la forma de transmisión de datos en tiempo real o transmisión periódica de archivos de datos a través del proceso por lotes. Revisión de los diagramas de flujo del sistema y código del sistema, y entrevista a los desarrolladores o administradores de la aplicación para

	obtener información sobre las interfaces y los controles de estas. Por ejemplo: los totales del control de las transmisiones de interfaz, ejemplo: totales de comprobación (*Hash*).
Tema 2 de auditoría: Preparación y validación de la información fuente ¿Es adecuada la gestión de documentos fuente, recopilación e ingreso de datos?	
Criterios: Los procedimientos de preparación de datos son documentados y comprendidos por los usuarios; existen registros adecuados de los documentos fuente recibidos hasta su eliminación; se asigna un número único y secuencial a cada registro; y se conservan los documentos fuente por el tiempo requerido por las políticas y normas legales.	
Información Requerida	**Método(s) de Análisis**
Procedimientos de preparación de datos fuente y validación. Actas de validación y registros de revisión de datos. Clases de documentos fuente. Criterio de la entidad para la puntualidad, integridad y exactitud de los documentos fuente. Interfaces de datos con otras aplicaciones. Políticas de conservación de documentos. Diagramas de flujo del sistema.	1. Comprobar la existencia de procedimientos documentados para preparar y validar la información fuente antes de su ingreso al sistema, confirmando que se definan responsabilidades, pasos de revisión y mecanismos de aprobación; para ello, se revisan manuales operativos, instructivos de ingreso de datos y actas de validación; como evidencia, buscar procedimientos firmados, flujogramas de revisión y registros de validación de información. 2. Revisión y observación de la elaboración y documentación de los procedimientos de preparación de datos, y consultar y confirmar si se comprenden los procedimientos y se utilizan los medios de fuente correctos. 3. Verificar que todos los documentos fuente incluyan elementos estandarizados, contengan documentación apropiada (por ejemplo, los códigos de entrada predeterminados, valores por defecto) y que estén autorizados por la gerencia. 4. Verificar que los documentos fuente críticos estén pre-enumerados y de qué manera se identifican y se abordan los números fuera de secuencia. Identificar y revisar los números fuera de secuencia, brechas y duplicaciones utilizando herramientas automatizadas (CAAT). Verificar si se asigna un número único y secuencial a cada registro a fin de evitar la duplicación. 5. Consultar al personal pertinente sobre las políticas de conservación. Verificar de qué manera se garantizan estas políticas. Se podría cotejar una muestra de los registros del sistema con los documentos fuente.

<table>
<tr><td colspan="2">Tema 3 de auditoría: Manejo de errores en la gestión de los datos
¿Cuenta la aplicación con procedimientos adecuados para el manejo de errores?</td></tr>
<tr><td colspan="2">Criterios:
Existe un sistema de mensajes de error claros y concisos que comunican los problemas a fin de que se puedan aplicar medidas correctivas inmediatas para cada tipo de error. Los errores son corregidos o debidamente eliminados antes del procesamiento de registros. Se revisan los registros periódicamente y se toman las medidas correctivas necesarias.</td></tr>
<tr><td>Información Requerida</td><td>Método(s) de Análisis</td></tr>
<tr><td>Tipos y mensajes de error

Procedimientos de revisión de registros

Políticas y procedimientos para abordar datos rechazados

Procedimientos de revisión de archivos transitorios.</td><td>1. Discutir el manejo de errores en la aplicación y excepciones con el desarrollador y/o administrador. Consultar y confirmar si existen políticas y procedimientos para el manejo de registros que no cumplen con los controles de edición y validación.
2. Verificar si el sistema proporciona mensajes de error para cada tipo de error (a nivel de campo o nivel de registro) que no cumpla con la validación de edición.
3. Verificar de qué manera la aplicación actúa si los datos son rechazados por los controles de entrada. Verificar si las partidas de datos son registradas o si se guardan automáticamente en un archivo transitorio. Verificar si el archivo transitorio automatizado incluye códigos que indican los tipos de errores, la fecha y hora de entrada, e identificar el usuario que ingresa los datos. Evaluar si existen procedimientos para la revisión y corrección de los datos en el archivo transitorio antes de procesarlos nuevamente. Evaluar si existe un procedimiento de escalada cuando la tasa de errores es demasiado alta y si se toman medidas correctivas.
4. Consultar a los gerentes si existen procedimientos para revisar periódicamente el registro. Verificar si los procedimientos incluyen el inicio de medidas correctivas. Obtener evidencia, ya sea documental o digital, de que el registro se revisa periódicamente.</td></tr>
<tr><td colspan="2">Tema 4 de auditoría: Autorizaciones de ingreso de datos
¿De qué manera se gestiona la autorización del ingreso de datos en la aplicación?</td></tr>
<tr><td colspan="2">Criterios:
Se establecieron niveles de autorización para el ingreso de datos y estos se aplican mediante controles adecuados existe una adecuada división de funciones para el ingreso de datos; existen controles compensatorios para aquellos casos en los que no es posible la división de funciones.</td></tr>
</table>

Información Requerida	Método(s) de Análisis
Requerimientos de cumplimiento legales y externos Requerimientos y reglas del negocio Manuales del usuario	1. Consultar y confirmar si el diseño del sistema contempla el uso de registros de autorización pre-aprobadas o concedidas. Verificar, mediante la revisión de listas de autorización, que los niveles de autorización estén adecuadamente definidos para cada grupo de registros. Evaluar si las reglas de autorización para el ingreso, edición, aceptación, rechazo y anulación de datos para los principales tipos de registros están bien elaboradas y documentadas. 2. Confirmar que los usuarios tengan roles o permisos claramente definidos para el ingreso de datos, garantizando que solo perfiles autorizados puedan registrar o modificar información; para ello, se revisan matrices de roles, configuraciones de permisos y bitácoras de control de acceso; como evidencia, buscar listados de usuarios autorizados, logs de acceso y registros de autorización. 3. Verificar que los niveles de autorización se apliquen adecuadamente mediante la ejecución de la aplicación en un entorno de pruebas. Verificar, mediante el uso de CAAT o módulos de auditoría incorporados, que los registros de autorización presentes en la base de datos cumplan con las normas de autorización establecidas. 4. Determinar si existe un cuadro para la división de funciones y verificar que existan una división de funciones/tareas clave adecuada y operaciones permitidas; a continuación, verificar la lista de usuarios y privilegios de acceso para cada usuario específico. Evaluar si la división de funciones garantiza que la persona que ingresa los datos no sea también responsable de la verificación de los documentos. Verificar la adopción de los controles compensatorios en los casos en que la división de funciones no sea factible.

7.2 Controles de Procesamiento
Objetivo de auditoría: Evaluar si la aplicación garantiza la integridad, la validez y la confiabilidad de los datos durante el ciclo de procesamiento de registros.
Tema 5 de auditoría: Diseño de los controles de procesamiento ¿Están las reglas y requerimientos del negocio correctamente internalizados en la aplicación?
Criterios: Las operaciones de la aplicación se ejecutan según se espera.

Información Requerida	Método(s) de Análisis
Documentación de la aplicación Reglas y requerimientos del negocio Diagrama de flujo de datos Lista de las operaciones altamente críticas	1. Identificar los programas ejecutables en la aplicación mediante el análisis del diagrama de flujo de datos y compararlos con las normas de procesos del negocio definidas y establecidas. 2. Revisión de la documentación de la aplicación para verificar que sea aplicable y adecuada para la tarea. Cuando sea apropiado para operaciones críticas, revisar el código para confirmar que los controles en las herramientas y las aplicaciones funcionan conforme a su diseño. Procesar nuevamente una muestra representativa para verificar que las herramientas automatizadas funcionan según lo previsto. 3. Para transacciones altamente críticas, establecer un sistema de prueba que funcione como el sistema real. Procesar operaciones en el sistema de prueba para garantizar que las operaciones válidas sean procesadas adecuadamente y de manera oportuna.
Tema 6 de auditoría: Controles de integridad transaccional ¿Garantizan los controles de la aplicación la integridad de las operaciones?	
Criterios: La aplicación identifica correctamente los errores en las operaciones. La integridad de los datos se mantiene incluso durante interrupciones inesperadas en el procesamiento de las operaciones. Existe un mecanismo adecuado para el manejo de errores de procesamiento, revisión de los archivos transitorios y depuración.	
Información Requerida	**Método(s) de Análisis**
Documentación de diseño de la aplicación Reglas y requerimientos del negocio Código fuente Manuales funcionales y reglas de negocio documentadas. Resultados de pruebas de cálculos y operaciones. Configuraciones de totales	1. Verificar que el sistema realiza los cálculos y operaciones conforme a reglas de negocio documentadas, asegurando que se apliquen correctamente los parámetros y fórmulas definidas; para ello, se revisan manuales funcionales, reglas de negocio y resultados de pruebas de cálculo; como evidencia, buscar especificaciones de lógica, casos de prueba ejecutados y reportes de validación de cálculos. 2. Evaluar si la aplicación cuenta con controles de validación adecuados para garantizar la integridad del procesamiento. Revisión de la funcionalidad y del diseño para verificar la existencia de errores de secuencia y duplicación, verificación de integridad de referencia, controles, y totales de comprobación (hash). 3. Confirmar si las transacciones procesadas quedan registradas en bitácoras de auditoría, garantizando la trazabilidad de cada operación realizada por el sistema;

de verificación o hash total. Reportes de auditoría técnica y logs de control de integridad. Logs de transacciones procesadas y bitácoras de auditoría. Diagramas de flujo y documentación de procesamiento automático. Procedimientos de validación de integridad y control de errores. Configuraciones de alertas automáticas y reportes de incidentes. Actas de revisión funcional y técnica de la lógica del sistema. Procedimientos para manejo de excepciones y registros de resolución de errores.	para ello, se revisan logs de transacciones, bitácoras del sistema y reportes de actividad; como evidencia, buscar registros de auditoría, reportes de seguimiento y logs de operaciones. 4. Evaluar que el procesamiento sea automático y sus resultados sean consistentes, asegurando que se minimice la intervención manual y se eviten errores por manipulación; para ello, se revisan diagramas de flujo, documentación técnica y reportes de ejecución; como evidencia, buscar logs de procesamiento automático, resultados de pruebas y evidencias de revisión de resultados. 5. Analizar que se implementaron controles de integridad durante todo el ciclo de procesamiento, verificando que la información mantenga su consistencia de extremo a extremo; para ello, se revisan procedimientos de control de integridad, validaciones en el flujo de trabajo y reportes de control de errores; como evidencia, buscar registros de validación de integridad, evidencias de control de datos y reportes de verificación. 6. Revisar la existencia de alertas automáticas en caso de errores de procesamiento, asegurando que el sistema notifique fallas y permita la reacción oportuna; para ello, se revisan configuraciones de alertas, reportes de incidentes y registros de monitoreo; como evidencia, buscar logs de alertas generadas, reportes de seguimiento y bitácoras de incidentes. 7. Comprobar la existencia de revisiones funcionales y técnicas de la lógica implementada en el sistema, confirmando que se hayan realizado verificaciones previas y posteriores a la puesta en operación; para ello, se revisan actas de revisión, reportes de auditoría técnica y registros de pruebas de validación; como evidencia, buscar actas firmadas, informes de verificación de lógica y registros de pruebas aprobadas. 8. Evaluar el tratamiento de excepciones durante el procesamiento de transacciones críticas, asegurando que existan procedimientos claros para manejar errores, reintentos y correcciones; para ello, se revisan procedimientos operativos, bitácoras de errores y reportes de incidencias; como evidencia, buscar procedimientos documentados, registros de seguimiento de excepciones y reportes de resolución. 9. Tomar una muestra de las operaciones de ingreso de datos.

	Utilizar un análisis y herramientas de búsqueda automatizados y apropiados para identificar casos en los que se identificaron errores equivocadamente y casos en los que los errores no fueron detectados. 10. Consultar y confirmar si hay funcionalidades que mantienen automáticamente la integridad de los datos ante las interrupciones inesperadas en el procesamiento de datos.

7.3 Controles de datos de Salida	
Objetivo de auditoría: evaluar si la aplicación garantiza que la información de salida sea completa y precisa antes de proseguir con su uso y que esté debidamente protegida.	
Tema 7 de auditoría: ¿Cuenta la aplicación con controles para garantizar la integridad y exactitud de los datos de salida?	
Criterios: Se han diseñado procedimientos para garantizar que se validen la integridad y exactitud de los datos de salida de la aplicación antes de que sean utilizados para el procesamiento posterior, incluido el uso en el procesamiento de usuarios finales; se permite la realización del seguimiento de los datos de salida de la aplicación; se verifican los datos de salida para corroborar su razonabilidad y exactitud; y los controles de integridad y precisión son eficaces.	
Información Requerida	**Método(s) de Análisis**
Reportes generados por el sistema y registros de transacciones. Especificaciones de reportes y cronogramas de emisión. Procedimientos de revisión y actas de aprobación de reportes. Formatos de reportes con controles de verificación y numeración. Registros de distribución de reportes y listas de destinatarios. Procedimientos de	1. Verificar que los reportes generados por el sistema reflejen fielmente los datos procesados, asegurando que la información final corresponda a los registros originales sin alteraciones; para ello, se revisan reportes generados, registros de transacciones y resultados de validación de consistencia; como evidencia, buscar reportes de prueba, registros de auditoría y evidencias de control de calidad. 2. Confirmar que los reportes sean completos, precisos y generados de forma oportuna, verificando que incluyan todos los datos requeridos dentro de los plazos establecidos; para ello, se revisan especificaciones de reportes, cronogramas de generación y registros de entrega; como evidencia, buscar reportes emitidos, registros de tiempos de ejecución y actas de conformidad. 3. Evaluar que existan mecanismos para revisar y aprobar reportes antes de su distribución, garantizando que se realicen controles de validación técnica y funcional; para ello, se revisan procedimientos de revisión, actas de aprobación y bitácoras de control; como evidencia, buscar registros de revisiones firmadas, listas de verificación y reportes aprobados. 4. Revisar que los reportes contengan controles como sumas de verificación o numeración de páginas, asegurando la

conciliación de datos y registros de validación.	integridad y completitud del contenido; para ello, se revisan formatos de reportes, configuraciones de plantilla y resultados de validación; como evidencia, buscar reportes con controles aplicados, ejemplos de numeración y pruebas de consistencia. 5. Verificar que existan procedimientos para conciliar datos de entrada y salida, confirmando que se realicen verificaciones de coherencia para detectar inconsistencias; para ello, se revisan procedimientos de conciliación, registros de revisiones cruzadas y reportes de control; como evidencia, buscar matrices de conciliación, registros de validación y actas de cierre de revisión.
Tema 8 de auditoría: Protección de los datos de Salida ¿Los datos de salida están protegidos adecuadamente?	
Criterios: La salida de datos se maneja de acuerdo con la clasificación de confidencialidad aplicable; la distribución de los datos de salida/los informes se controlan adecuadamente.	
Información Requerida	**Método(s) de Análisis**
Políticas de seguridad de información y matrices de permisos de acceso. Logs de acceso a reportes sensibles y registros de monitoreo. Manejo de datos de salida y procedimientos de conservación Políticas de clasificación de la información	1. Confirmar que los reportes que contienen información sensible tengan restricciones de acceso adecuadas, garantizando que se respete la confidencialidad y seguridad de los datos; para ello, se revisan políticas de seguridad, matrices de permisos y registros de control de acceso; como evidencia, buscar listas de usuarios autorizados, logs de acceso y registros de monitoreo. 2. Comprobar que la distribución de los reportes está controlada y documentada, asegurando que se entregue solo a usuarios autorizados y se registre la entrega; para ello, se revisan registros de distribución, listas de destinatarios y bitácoras de entrega; como evidencia, buscar reportes de distribución firmados, listas de control de envío y registros de recepción. 3. Revisar los procedimientos de manejo y conservación de los datos de salida para verificar su confidencialidad y seguridad. 4. Evaluar si se han establecido procedimientos que requieren el registro de errores potenciales y su resolución previo a la distribución de los informes. 5. Examinar el sistema de conciliación de los totales del control de los datos de salida por lotes con los totales de control de los datos de entrada por lotes antes de la presentación de los informes que determinan la integridad de los datos. 6. Verificar si se dispone de procedimientos documentados para

	el etiquetado de los datos de salida sensibles de la aplicación y, cuando sea necesario, enviar datos de salida sensibles a dispositivos de salida especiales con control de acceso. 7. Revisar los métodos de distribución de información sensible y verificar que los mecanismos procuren la implementación correcta de los derechos de accesos preestablecidos.

7.4 Controles de seguridad de aplicaciones	
Objetivo de auditoría: Evaluar si la información de la aplicación está correctamente resguardada contra el uso inadecuado.	
Tema 9 de auditoria: Trazabilidad de las acciones de usuarios ¿Son los mecanismos de trazabilidad de la aplicación suficientes para su propósito?	
Criterios: Se cuenta con perfiles de acceso, y existen pistas de auditoría que captan autorizaciones para las ediciones, anulaciones y registros de aprobaciones para las operaciones críticas, se promueve la segregación de funciones; se protegen los datos en el estado que se encuentren, y se registran pistas de auditoría para detectar actividad inusual; las pistas de auditoría son adecuadamente conservadas y protegidas; se asignan a cada registro números únicos y secuenciales, o identificadores.	
Información Requerida	**Método(s) de Análisis**
Matrices de roles y perfiles de acceso. Manuales de configuración de autenticación y políticas de autorización. Configuraciones de cifrado y certificados de seguridad (SSL/TLS). Logs de accesos, bitácoras de actividad y reportes de monitoreo. Matrices de segregación de	1. Verificar que existan perfiles de acceso claramente definidos y documentados, asegurando que cada rol cuente con permisos acordes a sus responsabilidades; para ello, se revisan matrices de roles, manuales de configuración de accesos y registros de autorización; como evidencia, buscar listas de perfiles aprobados, diagramas de roles y autorizaciones firmadas. 2. Revisar que se apliquen mecanismos de autenticación y autorización, confirmando que el sistema implemente controles para validar la identidad de los usuarios y restringir accesos según privilegios definidos; para ello, se revisan configuraciones de autenticación, políticas de acceso y bitácoras de control; como evidencia, buscar registros de configuración, logs de autenticación y reportes de pruebas de seguridad. 3. Evaluar que los datos sensibles y privados estén protegidos en tránsito y en reposo mediante cifrado u otros medios de seguridad que aseguren la confidencialidad e integridad de la información, según lo disponga la política de seguridad de la información y de clasificación de datos;

funciones y registros de asignación de roles. Formularios de solicitud de cambios de acceso y registros de aprobación. Configuraciones de detección de incidentes y procedimientos de respuesta. Cronogramas de revisiones periódicas y reportes de resultados. Actas de comités de seguridad y registros de ajustes de permisos. Estructura y documentación de las pistas de auditoría	para ello, se revisan configuraciones de cifrado, certificados de seguridad y reportes de auditoría técnica; como evidencia, buscar registros de políticas de cifrado, certificados SSL/TLS y validaciones de cumplimiento. 4. Comprobar la existencia de registros de accesos y su monitoreo periódico, asegurando la trazabilidad de las actividades de los usuarios en la aplicación; para ello, se revisan logs de acceso, reportes de monitoreo y bitácoras de actividad; como evidencia, buscar registros históricos de accesos, reportes de revisión periódica y evidencias de seguimiento. 5. Verificar que exista segregación de funciones en operaciones críticas, confirmando que no se concentren permisos incompatibles en un mismo perfil o usuario; para ello, se revisan matrices de SoD (Segregation of Duties), configuraciones de perfiles y registros de autorización; como evidencia, buscar matrices firmadas, registros de asignación de roles y reportes de revisión de segregación. 6. Evaluar que los cambios en permisos de acceso estén debidamente autorizados, garantizando que toda modificación sea validada por la autoridad competente; para ello, se revisan solicitudes de cambio, registros de aprobación y logs de modificación; como evidencia, buscar formularios de autorización, flujos de aprobación y reportes de auditoría de cambios. 7. Revisar que el sistema incluya mecanismos para detectar e informar incidentes de seguridad, asegurando que existan alertas, reportes y procedimientos de respuesta; para ello, se revisan configuraciones de monitoreo, reportes de incidentes y procedimientos de gestión de eventos; como evidencia, buscar logs de incidentes, reportes de alertas y registros de seguimiento. 8. Confirmar la existencia de revisiones periódicas sobre los accesos a la aplicación, verificando que se evalúe la vigencia y pertinencia de los permisos asignados; para ello, se revisan cronogramas de revisión, actas de comité de seguridad y reportes de resultados; como evidencia, buscar listas de usuarios actualizadas, actas de revisión y registros de ajustes. 9. Consultar de qué manera se restringe el acceso a las pistas de auditoría. Verificar los derechos de acceso y los registros de acceso a los archivos de pistas de auditoría. Verificar si únicamente el personal seleccionado y autorizado tiene

	acceso a las pistas de auditoría. 10. Evaluar si la pista de auditoría está protegida contra modificaciones privilegiadas. 11. Verificar, en lo posible, el uso de recopilación automatizada de evidencia, si se está asignando un único identificador a cada registro.

Mgs. Jaqueline Vargas Camacho
DIRECTORA (E)

Quito:
Calle Mañosca 201 y Av. 10 de Agosto
Atención ciudadana
Telf.: 3941-800
Ext.: 3134

www.registroficial.gob.ec

NGA/FMA

El Pleno de la Corte Constitucional mediante Resolución Administrativa No. 010-AD-CC-2019, resolvió la gratuidad de la publicación virtual del Registro Oficial y sus productos, así como la eliminación de su publicación en sustrato papel, como un derecho de acceso gratuito de la información a la ciudadanía ecuatoriana.

"Al servicio del país desde el 1º de julio de 1895"

El Registro Oficial no se responsabiliza por los errores ortográficos, gramaticales, de fondo y/o de forma que contengan los documentos publicados, dichos documentos remitidos por las diferentes instituciones para su publicación, son transcritos fielmente a sus originales, los mismos que se encuentran archivados y son nuestro respaldo.