PLAN ESTRATÉGICO TECNOLOGÍAS DE LA INFORMACIÓN
CONTRALORÍA DISTRITAL DE CARTAGENA DE INDIAS

ALCIBALDO ENRIQUE SEGUNDO CRUZ LEON

CONTRALOR DISTRITAL DE CARTAGENA DE INDIAS(D)

MANUEL CASSIANI CAÑATE y JAY MONTESINO UPARELA

PROCESO DE TECNOLOGIAS DE LA INFORMACION Y LAS COMUNICACIONES

CONTENIDO

Introducción 5

Misión y Visión del proceso de TI 7

Misión 7

Visión 8

Principios y Valores del Área de TI 9

Diagnóstico Situacional 10

Análisis Interno 10

Análisis Externo 13

Análisis FODA 14

Conclusiones del Diagnóstico 14

Objetivos Estratégicos del PETI 15

Mejorar la Infraestructura Tecnológica y de Conectividad 15

Fortalecer la Seguridad de la Información y Protección de Datos 16

Desarrollar y Mejorar los Sistemas de Información para el Control Fiscal 16

Capacitar y Desarrollar Competencias en el Personal de TI 17

Fomentar la Interoperabilidad y Colaboración con otras Entidades Públicas 18

Plan de Acción y Proyectos Estratégicos 19

Proyecto 1: Renovación de Infraestructura Tecnológica y Optimización de Redes 19

Proyecto 2: Fortalecimiento de la Seguridad de la Información y Protección de Datos 19

Proyecto 3: Implementación de un Sistema de Gestión Documental 20

Proyecto 4: Capacitación y Desarrollo de Competencias en TI 21

Proyecto 5: Integración e Interoperabilidad con otras Entidades Públicas 22

Proyecto 6: Desarrollo de Aplicativos de Software In-House para Apoyo a las labores misionales 23

Indicadores de Desempeño y Seguimiento 24

Indicadores para la Renovación de Infraestructura Tecnológica y Optimización de Redes 24

Indicadores para el Fortalecimiento de la Seguridad de la Información y Protección de Datos 24

Indicadores para el Sistema de Gestión Documental 25

Indicadores para Capacitación y Desarrollo de Competencias en TI 25

Indicadores para la Interoperabilidad con otras Entidades Públicas 25

Indicadores para el desarrollo de Aplicativos de Software In-House para Apoyo a las labores misionales 26

Cronograma de Implementación 26

Asignación de Recursos 27
Recursos Humanos 27
Recursos Financieros 27
Recursos Tecnológicos 27
Gestión de Riesgos 28
Identificación de Riesgos 28
Estrategias de Mitigación 29
Evaluación y Revisión del PETI 60
Evaluación del Desempeño 60
Revisión del PETI 61

INTRODUCCION

El Plan Estratégico de Tecnologías de Información (PETI) surge como respuesta a la necesidad de la Contraloría Distrital de Cartagena de Indias de modernizar sus recursos tecnológicos y optimizar sus procesos de control fiscal. En un contexto de creciente digitalización, donde los recursos públicos requieren una gestión transparente y eficiente, el PETI pretende adaptar la entidad a los desafíos de la era digital, alineando sus objetivos estratégicos con las políticas nacionales y normativas de protección de datos y transparencia.

El Plan Estratégico de Tecnologías de Información (PETI) de la Contraloría Distrital de Cartagena de Indias tiene como objetivo principal definir y estructurar la manera en que las tecnologías de información serán utilizadas para fortalecer y optimizar las funciones de control fiscal, auditoría y vigilancia de los recursos públicos. El PETI busca:

- Facilitar la toma de decisiones: Utilizar herramientas de análisis de datos y sistemas de información que permitan a los directivos contar con información oportuna y precisa para tomar decisiones basadas en datos. Esto incluye desde el control de recursos hasta la vigilancia fiscal.
- Mejorar la transparencia y eficacia en los procesos misionales: Modernizar y fortalecer los sistemas de procesos misionales para que los ciudadanos tengan mayor acceso a la información pública, promoviendo la transparencia. Esto también ayuda a mejorar la rendición de cuentas en la gestión de los recursos públicos.
- Fortalecer la seguridad de la información: Implementar políticas y herramientas avanzadas de ciberseguridad para proteger los datos personales y cumplir con normativas de protección de datos, como la Ley 1581 de 2012 en Colombia. La Contraloría manejará de manera confidencial y segura los datos que procesa y almacena.
- Modernizar la infraestructura tecnológica: Este objetivo responde a la necesidad de actualizar la infraestructura tecnológica de la entidad, que incluye hardware, software y redes, para que los sistemas de la Contraloría Distrital de Cartagena de Indias sean eficientes y sostenibles. También se evalúa la posibilidad de migrar ciertos servicios a la nube, lo que proporcionaría mayor flexibilidad y reducción de costos de almacenamiento y mantenimiento.
- Adoptar tecnologías emergentes: Explorar y aplicar tecnologías como big data, inteligencia artificial y blockchain que permitan mejorar los procesos de auditoría y control, optimizando la identificación de patrones y detección de irregularidades en la gestión de recursos.

El PETI también establece una hoja de ruta para la adopción de tecnologías emergentes que contribuyan a una transformación digital efectiva en la Contraloría Distrital de Cartagena de Indias. En suma, el objetivo es alinear la tecnología con las metas estratégicas de la entidad para maximizar su impacto en la gestión pública y contribuir a la transparencia.

Alcance

El alcance del PETI incluye todas las áreas operativas y administrativas de la Contraloría Distrital de Cartagena de Indias que interactúan con sistemas de información o administran datos relevantes para el control fiscal. Los componentes clave del alcance son:

- Sistemas de Información y Plataformas Digitales: Optimización y actualización de los sistemas actuales, así como la implementación de nuevas herramientas de gestión documental y análisis de datos para apoyar las labores de vigilancia fiscal.
- Infraestructura Tecnológica: Modernización de hardware y mejora de la conectividad, garantizando que la infraestructura permita la ejecución eficiente de los sistemas. Esto incluye actualizar redes internas y asegurar un rendimiento estable de los sistemas.
- Gestión de Seguridad y Privacidad de Datos: Creación y actualización de políticas de seguridad para proteger los datos, tanto personales como institucionales, alineándose con normativas como la Ley 1581 de 2012 y estándares internacionales como ISO 27001.
- Capacitación y Gestión del Talento en TI: Capacitación continua del personal en competencias tecnológicas esenciales, para mejorar la eficacia y el uso de los sistemas de información y otras herramientas digitales.
- Relaciones Interinstitucionales en TI: Fomentar la interoperabilidad con otras entidades públicas para compartir información y colaborar en iniciativas de vigilancia y control fiscal. Este punto implica cumplir con la Política de Gobierno Digital del MinTIC, que prioriza la interconexión entre entidades.

Normatividad y Marco de Referencia

Para asegurar el cumplimiento de normativas y políticas nacionales, este PETI se enmarca en varias leyes, decretos y lineamientos, entre los cuales se destacan:

- Ley 1581 de 2012 - Protección de Datos Personales: Establece los principios y derechos para el tratamiento de datos personales en Colombia. La Contraloría debe asegurar que los datos utilizados en auditorías, vigilancia fiscal y cualquier otro proceso, cumplan con los principios de confidencialidad, seguridad y privacidad.
- Ley 1712 de 2014 - Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional: Esta ley establece que toda entidad pública debe garantizar el acceso a la información pública, promoviendo transparencia y facilitando el control ciudadano. En el contexto del PETI, se buscará un balance entre acceso a la información y protección de la misma.
- Política de Gobierno Digital del Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC): Define los lineamientos para la digitalización y modernización de las entidades públicas en Colombia, con énfasis en la interoperabilidad, la seguridad y la accesibilidad de los sistemas. El PETI debe adherirse a estas pautas para asegurar una integración efectiva con otras entidades públicas y fomentar la transparencia digital.

- Guía para la Gestión de Seguridad y Privacidad de la Información de Colombia: Proporciona lineamientos específicos para la protección
  de la información, especialmente relevante en la implementación de sistemas de auditoría y gestión de datos dentro de la Contraloría.
- Normas Internacionales de Auditoría y Control Fiscal (INTOSAI): Estas normas establecen pautas de auditoría y gestión de riesgos que pueden ser implementadas mediante tecnologías de información, elevando los estándares de control y evaluación fiscal.
- Decreto 1078 de 2015: También conocido como el Decreto Único Reglamentario del Sector TIC, establece reglas para la contratación de servicios de TI y la adopción de tecnologías en las entidades públicas, proporcionando una guía para la adquisición de recursos tecnológicos.

Beneficios Esperados

Al implementar este PETI, la Contraloría Distrital de Cartagena de Indias espera obtener múltiples beneficios:

- Eficiencia Operativa: Mejora de los tiempos de respuesta y la reducción de costos operativos mediante la automatización de procesos y el uso de herramientas digitales.
- Transparencia y Confianza Ciudadana: Incremento en la transparencia del proceso de control fiscal, lo cual contribuye a la confianza de la ciudadanía.
- Gestión Proactiva de la Información: Facilitar la gestión de riesgos y la toma de decisiones basadas en datos, fortaleciendo el monitoreo y control de los recursos públicos.
- Cumplimiento de la Normatividad Vigente: Asegurar que todos los procesos relacionados con el manejo de la información sean conformes con la normativa nacional e internacional en materia de TI y protección de datos.

MISIÓN Y VISIÓN DEL PROCESO DE TI

Misión

La misión del área de TI de la Contraloría Distrital de Cartagena de Indias se centra en proporcionar soluciones tecnológicas que no solo respalden, sino que impulsen el control fiscal, la auditoría y la vigilancia de los recursos públicos del distrito. Esto implica la gestión de los recursos tecnológicos en alineación con la misión institucional de la Contraloría Distrital de Cartagena de Indias, que busca garantizar la transparencia y eficiencia en el uso de los recursos públicos.

Desglose de los Componentes Clave de la Misión:

- Eficiencia en Procesos:
  - El área de TI tiene el compromiso de asegurar que los sistemas de información y plataformas tecnológicas sean eficientes, de fácil acceso y optimicen los tiempos de respuesta para los funcionarios y usuarios.
  - Esto se logra mediante la automatización de tareas repetitivas, lo cual permite que el personal de la Contraloría Distrital de Cartagena de Indias pueda enfocarse en

análisis más estratégicos y en actividades de mayor valor añadido para el control fiscal.

- Transparencia en la Gestión Pública:
  - La transparencia es fundamental en la gestión de la Contraloría Distrital de Cartagena de Indias. Por lo tanto, los datos y sistemas de información deben estar disponibles y accesibles de manera oportuna y segura, permitiendo que la información clave esté al alcance de todos los involucrados, desde ciudadanos hasta auditores.
  - Esto incluye la implementación de tecnologías que permitan la publicación de información y datos en tiempo real, facilitando la vigilancia y control ciudadano.
- Seguridad y Confiabilidad de la Información:
  - La seguridad de la información es un pilar en la misión del área de TI, ya que la Contraloría Distrital de Cartagena de Indias gestiona datos sensibles sobre la administración de los recursos públicos.
  - El área de TI está comprometida en la gestión de políticas y prácticas de ciberseguridad para proteger la integridad, disponibilidad y confidencialidad de estos datos. Esto incluye la adopción de estándares internacionales de seguridad, como la ISO 27001, y la aplicación de técnicas avanzadas de encriptación y control de accesos.
- Innovación y Modernización Continua:
  - La misión del área de TI también abarca la responsabilidad de mantenerse actualizada con las últimas tendencias y herramientas tecnológicas. Esto implica adoptar prácticas de innovación y modernización que permitan implementar sistemas avanzados, como el análisis de big data y la inteligencia artificial, para apoyar el análisis de datos en auditorías fiscales.
  - La adopción de nuevas tecnologías es vital para detectar irregularidades y patrones en grandes volúmenes de datos, lo cual facilita la proactividad en la vigilancia fiscal.

Visión

La visión del área de TI de la Contraloría de Cartagena de Indias es posicionarse como un área estratégica, reconocida por su capacidad de impulsar una transformación digital efectiva dentro de la institución. La visión subraya el papel de TI no solo como un soporte, sino como un motor de innovación que fortalece la misión de la Contraloría Distrital de Cartagena de Indias en el cumplimiento de sus objetivos de control y vigilancia.

Componentes Fundamentales de la Visión:

- Transformación Digital Efectiva:
  - La transformación digital busca elevar el nivel de eficiencia y automatización de los procesos de control y auditoría. La Contraloría Distrital de Cartagena de Indias busca liderar esta transformación adoptando herramientas avanzadas que no solo agilicen el flujo de trabajo, sino que también faciliten una gestión pública más accesible y transparente.

- El proceso de TI deberá implementar herramientas como la digitalización de documentos, gestión automatizada de
  auditorías, y sistemas de procesamiento de datos en tiempo real que optimicen las tareas de control.

- Infraestructura Tecnológica Robusta y Segura:
  - La visión incluye el establecimiento de una infraestructura tecnológica sólida que permita enfrentar los retos de seguridad y crecimiento a futuro. Esto significa que la infraestructura de TI debe estar preparada para soportar no solo las demandas actuales, sino también las crecientes amenazas de ciberseguridad.
  - La implementación de una infraestructura resiliente y de alta disponibilidad garantizará que la información y los sistemas críticos para la Contraloría Distrital de Cartagena de Indias estén protegidos contra accesos no autorizados y se mantengan operativos en situaciones de crisis.
- Promoción de la Interoperabilidad y Colaboración Interinstitucional:
  - La interoperabilidad y la integración de sistemas con otras entidades públicas, tanto a nivel distrital como nacional, son objetivos clave en la visión de TI. Esto se traduce en la creación de conexiones y canales de comunicación eficientes que permitan un flujo de información constante entre organismos.
  - Esta integración facilitará el trabajo conjunto con entidades gubernamentales, mejorando la vigilancia y el control de los recursos públicos, y permitirá que la Contraloría Distrital de Cartagena de Indias funcione como un nodo en una red de control fiscal interconectado.
- Referente en Buenas Prácticas de TI:
  - Finalmente, el proceso de TI busca consolidarse como un modelo de referencia en el uso de tecnologías de información dentro del sector público, aplicando estándares altos en la gestión de tecnologías y seguridad de la información.
  - La meta es que otras contralorías y entidades de control en el país puedan adoptar las prácticas de TI implementadas en Cartagena como ejemplos de eficiencia, transparencia y seguridad.

Principios y Valores del Área de TI

Para cumplir con su misión y visión, el proceso de TI se guía por una serie de principios y valores que moldean sus prácticas y decisiones estratégicas:

- Integridad:
  Este principio fomenta la honestidad y transparencia en todos los procesos de TI, asegurando un manejo ético de los recursos tecnológicos y la información que gestiona la Contraloría Distrital de Cartagena de Indias.
- Excelencia:

La excelencia implica un compromiso con la mejora continua en todos los aspectos del proceso de TI. Esto incluye adoptar y
mantener prácticas de alta calidad en el desarrollo, mantenimiento y operación de los sistemas tecnológicos.

- Seguridad:
  La protección de datos es prioritaria, y la seguridad en TI se enfoca en garantizar la confidencialidad, integridad y disponibilidad de la información. Este valor guía la implementación y actualización continua de mecanismos de seguridad que minimicen el riesgo de vulnerabilidades o accesos no autorizados.
- Innovación:
  El proceso de TI promueve un ambiente de innovación constante, buscando siempre soluciones tecnológicas avanzadas que permitan a la Contraloría Distrital de Cartagena de Indias alcanzar sus objetivos de forma más efectiva. Esto implica fomentar la adopción de tecnologías emergentes como el análisis de big data y la inteligencia artificial.
- Orientación al Usuario:
  Tanto para el personal interno como para los ciudadanos, la TI está orientada a proporcionar herramientas y servicios que mejoren la experiencia y faciliten la interacción con los sistemas de la entidad, promoviendo un acceso fácil y seguro a la información.
- Responsabilidad Social:
  Como parte de una entidad pública, el proceso de TI tiene una responsabilidad con la comunidad y la sociedad. El uso de recursos tecnológicos debe ser sostenible, ético y respetuoso de la privacidad y seguridad de los datos personales, contribuyendo al bienestar general y fortaleciendo la confianza de los ciudadanos en la Contraloría Distrital de Cartagena de Indias.

DIAGNÓSTICO SITUACIONAL

El diagnóstico situacional del proceso de Tecnologías de la Información de la Contraloría Distrital de Cartagena de Indias se basa en tres áreas principales: análisis interno, análisis externo y análisis FODA. Esto permite una evaluación integral del estado actual de los recursos tecnológicos y de su alineación con los objetivos estratégicos de la entidad.

Análisis Interno

El análisis interno examina la infraestructura tecnológica, sistemas de información, políticas de seguridad, y el nivel de competencias del personal de TI dentro de la Contraloría Distrital de Cartagena de Indias. Este enfoque permite identificar fortalezas y debilidades estructurales que impactan la capacidad operativa y la eficacia en el cumplimiento de sus funciones. Infraestructura Tecnológica

- Equipamiento y Hardware:
  Se ha identificado que una gran parte de los equipos de TI de la Contraloría Distrital de Cartagena de Indias son obsoletos, lo cual afecta directamente el rendimiento y la eficiencia de las operaciones. La falta de actualización de

hardware y la antigüedad de los equipos impactan negativamente en el procesamiento de información y en la velocidad de respuesta.

Existe una necesidad urgente de renovar tanto los servidores como los equipos de usuario final (computadoras de escritorio y portátiles), así como otros dispositivos clave. La actualización de estos dispositivos permitirá un rendimiento más eficiente y reducirá los tiempos de inactividad relacionados con fallos en el hardware.

- Conectividad y Redes:

  Las redes internas presentan limitaciones significativas, y no cuentan con el rendimiento ni la disponibilidad suficiente para soportar herramientas avanzadas de auditoría o sistemas en tiempo real.

  La infraestructura de conectividad requiere optimización para garantizar una conexión continua y de alta velocidad entre todos las recursos de la Contraloría Distrital de Cartagena de Indias, especialmente en el uso de aplicaciones críticas para el control fiscal. La optimización de esta infraestructura no solo mejoraría la velocidad de trabajo, sino que permitiría la implementación de sistemas de comunicación y colaboración más efectivos.

Sistemas de Información

- Software de Auditoría y Control Fiscal:

  El software actual utilizado para las auditorías es básico y limitado en sus funcionalidades. Esta carencia limita el análisis detallado de grandes volúmenes de datos y la capacidad para detectar patrones complejos en las auditorías fiscales.

  La implementación de una plataforma avanzada de auditoría permitiría realizar análisis más exhaustivos y detectar irregularidades de manera proactiva, incrementando la precisión y el alcance del control fiscal.

- Sistema de Gestión Documental:

  Actualmente, no existe un sistema de gestión documental robusto que permita la organización y el acceso eficiente a la información archivada. La gestión documental es clave para la transparencia y la eficiencia en la búsqueda y recuperación de datos históricos.

  La ausencia de este sistema implica que la información no está centralizada ni organizada adecuadamente, lo cual dificulta su manejo y su consulta rápida por parte del personal.

- Sistemas de Interoperabilidad:

  La falta de integración con plataformas de otras entidades gubernamentales representa una limitación importante para la Contraloría Distrital de Cartagena de Indias. La interoperabilidad entre sistemas permitiría un flujo de datos más eficiente, facilitando la colaboración con otras instituciones.

Sin esta integración, la Contraloría Distrital de Cartagena de Indias no puede acceder a información en tiempo real
de otras entidades, lo cual restringe la eficiencia de los procesos de auditoría y control fiscal.

Seguridad y Protección de Datos

- Políticas de Seguridad:
  Las políticas de seguridad de la información están en proceso de actualización para alinearse con las normativas de protección de datos, como la Ley 1581 de 2012. Sin embargo, se identifican carencias en áreas críticas, como el control de accesos, encriptación de datos y autenticación multifactor.
  La implementación de una política de seguridad robusta es esencial para proteger los datos confidenciales manejados por la Contraloría Distrital de Cartagena de Indias y reducir el riesgo de vulnerabilidades o ciberataques.
- Incidentes de Seguridad:
  La institución ha registrado varios incidentes de seguridad menores, lo cual indica una necesidad urgente de mejorar las medidas de protección y el monitoreo constante. La seguridad de la información es un aspecto crucial para la Contraloría Distrital de Cartagena de Indias, dado el tipo de datos que maneja.
  La frecuencia de estos incidentes señala la urgencia de implementar un sistema integral de ciberseguridad que incluya firewalls, sistemas de detección de intrusiones y protocolos de respuesta rápida ante incidentes.

Recursos Humanos y Competencias en TI

- Capacidades del Personal:
  El personal de TI posee conocimientos básicos en el uso de tecnologías, pero carece de experiencia en áreas avanzadas, como la seguridad de la información, gestión de datos y herramientas de auditoría.
  Esto implica que la Contraloría Distrital de Cartagena de Indias debe invertir en un programa de capacitación continua que permita al personal de TI actualizarse en competencias esenciales para el cumplimiento de sus funciones.
- Capacitación Continua:
  Existen muy pocas oportunidades de actualización tecnológica para el personal. La falta de capacitación y desarrollo limita la capacidad de la Contraloría Distrital de Cartagena de Indias para adaptarse a nuevas herramientas y metodologías.
  La implementación de un programa formal de capacitación en áreas clave como ciberseguridad, análisis de datos y gestión documental es crucial para mejorar las habilidades del personal y permitirles responder a las crecientes demandas tecnológicas.

Análisis Externo

Este análisis considera las tendencias tecnológicas, los estándares de la industria y las oportunidades externas de las que la Contraloría Distrital de Cartagena de Indias puede beneficiarse.

Tendencias Tecnológicas

- Inteligencia Artificial y Big Data:
  Estas tecnologías emergentes tienen un potencial significativo para la Contraloría Distrital de Cartagena de Indias. El uso de IA en auditorías permite analizar patrones y datos a gran escala, facilitando la detección de irregularidades que podrían pasar desapercibidas en los métodos tradicionales.
  Big data, por su parte, ofrece la posibilidad de manejar grandes volúmenes de información, permitiendo a la Contraloría Distrital de Cartagena de Indias mejorar la precisión de sus auditorías y el análisis de riesgos.
- Computación en la Nube:
  La migración a la nube puede proporcionar flexibilidad y reducir costos en almacenamiento, además de mejorar la accesibilidad y la colaboración entre equipos.
  Para la Contraloría Distrital de Cartagena de Indias, adoptar la computación en la nube significa una oportunidad para centralizar sus datos y facilitar el acceso remoto, optimizando así el trabajo colaborativo.
- Blockchain:
  Aunque esta tecnología aún está en fase de exploración en el sector público de Colombia, el blockchain podría ofrecer mayores garantías de transparencia y seguridad en los procesos de auditoría en el futuro.
  Esta tecnología podría asegurar que los datos de auditoría no sean manipulados y se mantengan inalterables, lo que sería beneficioso para la integridad de los procesos de la Contraloría Distrital de Cartagena de Indias.

Normativas y Buenas Prácticas

- Políticas Nacionales y Locales en TI:
  Las políticas nacionales impulsan la digitalización y modernización de las entidades públicas, y la Contraloría Distrital de Cartagena de Indias debe adherirse a estas normativas para asegurar un uso ético y seguro de la información.
  Esto incluye el cumplimiento de normativas como la Ley 1581 de 2012 (protección de datos personales) y la Ley 1712 de 2014 (acceso a la información pública), las cuales establecen pautas para la transparencia y seguridad de la información pública.
- Mejores Prácticas de Seguridad:

Los estándares de seguridad como ISO 27001 proporcionan pautas para desarrollar políticas y protocolos que protejan la información sensible.
La adopción de estas normas podría ayudar a la Contraloría Distrital de Cartagena de Indias a elevar sus estándares de seguridad y reducir la vulnerabilidad frente a amenazas cibernéticas.

Relaciones con otras Entidades Gubernamentales

La colaboración con otras entidades públicas a nivel distrital y nacional ofrece oportunidades para fortalecer la interoperabilidad y optimizar la eficiencia en los procesos de control fiscal.

Esta integración permitiría un intercambio de información más fluido y la colaboración en proyectos conjuntos, mejorando la capacidad de vigilancia de la Contraloría Distrital de Cartagena de Indias.

Análisis FODA
Fortalezas:

- Compromiso de la dirección para mejorar la infraestructura tecnológica y experiencia básica del personal en sistemas de información.
- Cultura de mejora continua en los procesos misionales y control, lo cual facilita la adopción de cambios tecnológicos y metodológicos.

Oportunidades:

- Los avances tecnológicos como IA y big data pueden mejorar la precisión en auditorías, permitiendo análisis más detallados y predictivos.
- Apoyo de entidades gubernamentales superiores y del MinTIC, que pueden proporcionar asistencia técnica y financiera en la modernización de la infraestructura tecnológica.

Debilidades:

- Infraestructura de TI obsoleta que afecta directamente el rendimiento de los sistemas y la eficiencia operativa.
- Falta de integración entre los sistemas internos y con otras plataformas gubernamentales, lo cual dificulta el intercambio de información y la colaboración interinstitucional.

Amenazas:

- Aumento de amenazas de ciberseguridad que pueden comprometer la integridad de la información fiscal y la confidencialidad de los datos.
- Dependencia de sistemas y proveedores externos sin control directo, lo cual representa un riesgo en términos de inoperabilidad y vulnerabilidad en la entrega de servicios.

Conclusiones del Diagnóstico
El diagnóstico situacional revela que la Contraloría Distrital de Cartagena de Indias está en una fase inicial de modernización tecnológica, con múltiples áreas críticas a mejorar, especialmente

en infraestructura, seguridad y desarrollo de competencias del personal.
Esta situación permite priorizar las acciones estratégicas y centrarse en los aspectos que generen el mayor impacto en la efectividad y transparencia de los procesos de control fiscal.

En resumen, el diagnóstico sitúa al PETI como una herramienta clave para la modernización tecnológica de la Contraloría Distrital de Cartagena de Indias, permitiendo planificar y estructurar las mejoras necesarias para que la entidad esté a la altura de las demandas tecnológicas y normativas actuales.

OBJETIVOS ESTRATÉGICOS DEL PETI

Con base en el diagnóstico situacional, se establecen los siguientes objetivos estratégicos para guiar el desarrollo de las Tecnologías de la Información en la Contraloría Distrital de Cartagena de Indias:

Mejorar la Infraestructura Tecnológica y de Conectividad

Este objetivo busca actualizar y optimizar la infraestructura de TI, incluyendo hardware, redes y conectividad, para garantizar un ambiente de trabajo que permita un uso óptimo de los sistemas de auditoría, control y gestión documental. Una infraestructura moderna y bien gestionada es esencial para asegurar que la Contraloría Distrital de Cartagena de Indias opere de manera eficiente y pueda responder a las demandas actuales y futuras.

Indicadores:

- Porcentaje de equipos renovados: Refleja el progreso en la renovación del hardware de TI, como estaciones de trabajo, servidores y otros equipos críticos.
- Disponibilidad de red: Mide la estabilidad y tiempo de operación de la red y conectividad interna sin interrupciones, expresado como porcentaje de disponibilidad mensual.
- Tiempo de respuesta de los sistemas: Evalúa la eficiencia del sistema, midiendo la reducción en los tiempos de carga y procesamiento en aplicaciones críticas.

Acciones Clave:

- Adquisición y Renovación de Hardware:
  Sustitución de equipos obsoletos y adquisición de hardware moderno y compatible con las necesidades tecnológicas de la Contraloría Distrital de Cartagena de Indias. Esto incluye la actualización de servidores y dispositivos de usuario final, que son cruciales para un rendimiento óptimo y la continuidad de los procesos de auditoría y control.
- Optimización de la Infraestructura de Redes Internas:
  Mejorar la conectividad en oficina, asegurando una red estable y de alta velocidad para mantener una comunicación fluida y acceso constante a los sistemas de información.
- Evaluación de Migración a la Nube:
  Considerar la posibilidad de trasladar ciertos servicios o sistemas a la nube para mejorar la accesibilidad, reducir costos de almacenamiento y facilitar el trabajo colaborativo. La

migración a la nube permitiría un acceso remoto seguro y eficiente a los recursos y datos necesarios para las auditorías.

Fortalecer la Seguridad de la Información y Protección de Datos

La seguridad de la información es fundamental para proteger la integridad, confidencialidad y disponibilidad de los datos manejados por la Contraloría Distrital de Cartagena de Indias. Este objetivo busca implementar políticas y medidas de seguridad que aseguren el cumplimiento de la normativa en protección de datos personales y resguarden la información de la entidad contra ciberamenazas.

Indicadores:

- Número de incidentes de seguridad reportados y solucionados: Este indicador mide la reducción de incidentes y la capacidad de respuesta ante vulnerabilidades en el sistema.
- Nivel de cumplimiento de la Política de Tratamiento de Datos Personales: Evalúa la conformidad de las políticas de manejo de datos en relación con la normativa vigente, como la Ley 1581 de 2012.
- Porcentaje de personal capacitado en seguridad digital: Mide la cantidad de empleados formados en prácticas de seguridad, lo cual es clave para una cultura de ciberseguridad en toda la entidad.

Acciones Clave:

- Desarrollo de Políticas de Seguridad de la Información:
  Formular e implementar políticas de seguridad alineadas con estándares internacionales, como ISO 27001, que aseguren la protección de los datos sensibles y la continuidad de los servicios de TI.
- Implementación de Controles de Seguridad:
  Adoptar medidas de seguridad avanzada, tales como autenticación multifactor, encriptación de datos y sistemas de detección y prevención de intrusiones (IDS/IPS). Estos controles mejoran significativamente la protección contra accesos no autorizados y ciberataques.
- Capacitación y Sensibilización en Seguridad de la Información:
  Realizar campañas de concientización y capacitaciones periódicas para todo el personal en prácticas de seguridad digital, con el fin de crear una cultura de ciberseguridad que minimice los riesgos derivados de errores humanos o prácticas inseguras.

Desarrollar y Mejorar los Sistemas de Información para el Control Fiscal

Este objetivo se enfoca en optimizar y expandir las capacidades de los sistemas de información, de modo que la Contraloría Distrital de Cartagena de Indias pueda realizar auditorías, control y análisis de datos de manera más efectiva y con base en evidencia. El desarrollo de estos sistemas contribuirá a la precisión en el monitoreo de los recursos públicos y facilitará la detección de patrones y posibles irregularidades.

Indicadores:

- Reducción en el tiempo de realización de auditorías e informes: Mide la eficiencia en la realización de auditorías y en la generación de informes gracias a los sistemas mejorados.
- Grado de automatización en los procesos de auditoría: Indica el nivel de automatización de tareas repetitivas y de bajo valor añadido, permitiendo que los auditores se concentren en análisis estratégicos.
- Aumento en la capacidad de análisis de datos y detección de patrones: Evalúa la efectividad de las herramientas de análisis implementadas para identificar irregularidades y mejorar el control fiscal.

Acciones Clave:

- Implementación de un Sistema de Gestión Documental:
  Crear un sistema que permita una organización y búsqueda eficiente de la información, facilitando el acceso a documentos relevantes para auditorías y revisiones.
- Incorporación de Herramientas de Análisis de Datos:
  Adquirir o desarrollar herramientas avanzadas de análisis de datos que permitan procesar grandes volúmenes de información, facilitando el análisis predictivo y la identificación de patrones de riesgo en el uso de recursos.
- Integración de Sistemas Internos con Plataformas Gubernamentales:
  Mejorar la interoperabilidad de los sistemas de la Contraloría con otras plataformas gubernamentales, promoviendo el flujo seguro y eficiente de información y fortaleciendo la colaboración interinstitucional.

Capacitar y Desarrollar Competencias en el Personal de TI
Este objetivo tiene como propósito asegurar que el personal de TI y de otras áreas cuente con las habilidades y conocimientos necesarios para maximizar el uso de las herramientas tecnológicas y para gestionar los recursos tecnológicos de la Contraloría Distrital de Cartagena de Indias. La capacitación continua es crucial para mantener al equipo actualizado en prácticas modernas y tendencias en TI.

Indicadores:

- Número de capacitaciones anuales realizadas: Mide el progreso en la implementación del programa de capacitación, asegurando que el personal reciba formación relevante y continua.
- Evaluaciones de competencia y habilidades del personal en TI: Evalúa el impacto de las capacitaciones y el nivel de competencia alcanzado por el personal, indicando si las formaciones son efectivas y útiles.
- Satisfacción de los usuarios respecto al soporte y formación en TI: Refleja la percepción del personal sobre la calidad y utilidad de las capacitaciones, lo que ayuda a ajustar los contenidos y metodologías de enseñanza.

Acciones Clave:

- Diseño de un Programa de Capacitación Continua:
  Crear un programa de formación que aborde temas clave como seguridad de la información, análisis de datos y gestión de sistemas. Esto incluye capacitaciones periódicas y certificaciones en áreas estratégicas.
- Promover Certificaciones en Ciberseguridad y Gestión de Proyectos:
  Incentivar la obtención de certificaciones internacionales (como CompTIA, CISSP, ITIL, PRINCE2, CISM o PMP) para fortalecer las capacidades técnicas y de gestión del equipo de TI, asegurando que el personal esté capacitado en áreas críticas.
- Fomento de una Cultura de Innovación:
  Establecer un ambiente de aprendizaje y actualización constante para que el personal de TI esté al día con las nuevas tendencias y adopte soluciones innovadoras que potencien la eficacia de los sistemas y recursos.

Fomentar la Interoperabilidad y Colaboración con otras Entidades Públicas
Este objetivo tiene como finalidad facilitar la interoperabilidad y la colaboración entre la Contraloría Distrital de Cartagena de Indias y otras entidades gubernamentales para optimizar el uso de los recursos y mejorar la eficiencia en el control fiscal y la vigilancia de los recursos públicos. Una colaboración efectiva permitirá un flujo de información ágil y seguro, beneficiando la transparencia y eficiencia del control fiscal.

Indicadores:

- Número de sistemas interoperables con otras entidades: Refleja el grado de integración de los sistemas de la Contraloría Distrital de Cartagena de Indias con plataformas de otras entidades, facilitando el intercambio de datos.
- Reducción en el tiempo de obtención de información externa para auditorías: Mide la rapidez en la que se accede a datos externos gracias a la interoperabilidad, acelerando los tiempos de respuesta.
- Grado de colaboración en proyectos conjuntos: Indica la frecuencia y éxito de la cooperación en iniciativas compartidas con otras entidades, como auditorías conjuntas o proyectos de análisis de datos.

Acciones Clave:

- Establecimiento de Estándares de Interoperabilidad:
  Definir y aplicar estándares de integración que permitan el intercambio seguro y eficaz de información con otras plataformas gubernamentales, asegurando una comunicación fluida y en tiempo real.
- Desarrollo de Interfaces de Intercambio de Datos:
  Crear y optimizar conexiones seguras con entidades gubernamentales clave, permitiendo una colaboración más efectiva y una gestión ágil de la información fiscal.
- Promoción de Proyectos de Colaboración Interinstitucional:

Fomentar acuerdos de colaboración y proyectos compartidos en TI con otras contralorías y organismos públicos. Esto incluye el
desarrollo de plataformas conjuntas y la creación de programas de trabajo en común para la vigilancia de recursos.

PLAN DE ACCIÓN Y PROYECTOS ESTRATÉGICOS

El plan de acción incluye proyectos clave para cumplir con los objetivos estratégicos del PETI. Cada proyecto se estructura en actividades específicas, plazos estimados, responsables y recursos requeridos.

Proyecto 1: Renovación de Infraestructura Tecnológica y Optimización de Redes
Objetivo: Modernizar el hardware, software y la infraestructura de red para mejorar el rendimiento, disponibilidad y seguridad de los sistemas de la Contraloría Distrital de Cartagena de Indias.

Actividades:

- Evaluación y priorización de equipos críticos: Identificar los equipos y servidores con más antigüedad y priorizar su renovación para evitar problemas de rendimiento y seguridad.
- Implementación de una red privada virtual (VPN): Establecer una VPN para el personal autorizado, permitiendo el acceso seguro desde ubicaciones remotas y asegurando el cifrado de los datos.
- Monitoreo continuo de red y mantenimiento preventivo: Configurar herramientas de monitoreo en tiempo real, como SolarWinds o Nagios, para detectar problemas de red y llevar a cabo mantenimiento preventivo mensual.
- Migración de servidores a la nube: Evaluar una migración parcial o total de los servidores de la Contraloría a una plataforma en la nube para optimizar el acceso y reducir los costos de infraestructura.

Responsables: Equipo de TI, con apoyo de proveedores

externos. Recursos:

- Financieros: Presupuesto para adquisición de hardware y servicios en la nube.
- Humanos: Personal de TI y consultores especializados en redes.
- Tecnológicos: Licencias de software, dispositivos de red.

Proyecto 2: Fortalecimiento de la Seguridad de la Información y Protección de Datos
Objetivo: Implementar medidas robustas de seguridad y garantizar el cumplimiento de la normativa de protección de datos.

Actividades:

- Desarrollo de políticas de seguridad de la información: Crear políticas alineadas con ISO 27001 y regulaciones locales.
- Instalación de herramientas de ciberseguridad: Firewalls, autenticación multifactor, y sistemas de detección de intrusiones.
- Capacitación en seguridad de la información: Capacitar a todos los colaboradores en prácticas seguras.
- Evaluación y clasificación de datos: Realizar un inventario de la información y clasificarla según su nivel de sensibilidad, aplicando controles de acceso basados en esta clasificación.
- Desarrollo de un plan de respuesta a incidentes (PRI): Crear un PRI con procedimientos detallados para la detección, contención y resolución de incidentes de seguridad.
- Integración de un sistema SIEM (Security Information and Event Management): Implementar un sistema SIEM, como Splunk o IBM QRadar, que permita la recolección y análisis de eventos de seguridad en tiempo real para detectar amenazas.
- Auditorías de seguridad trimestrales y pruebas de penetración: Programar auditorías internas y pruebas de penetración realizadas por un equipo especializado para identificar y mitigar vulnerabilidades.

Responsables: Proceso de Tecnologías de la Información y las Comunicaciones, en colaboración con el área de Talento Humanos para la capacitación.

Recursos:

- Financieros: Presupuesto para herramientas de ciberseguridad.
- Humanos: Personal del proceso de Tecnologías de la Información y las Comunicaciones y capacitadores en ciberseguridad.
- Tecnológicos: Software de seguridad y licencias.

Proyecto 3: Implementación de un Sistema de Gestión Documental Digital
Objetivo: Crear un sistema de gestión documental que facilite el acceso, la organización y la seguridad de los archivos institucionales.

Actividades:

- Selección de software de gestión documental: Evaluación y adquisición del sistema adecuado.
- Migración de documentos existentes: Digitalización y organización en el nuevo sistema.
- Capacitación del personal en el uso del sistema: Formar a los colaboradores en el manejo de la plataforma.

- Definición de estándares de digitalización: Establecer estándares de calidad para la digitalización de documentos, asegurando que todos los archivos escaneados sean legibles y de alta calidad.
- Creación de una política de retención documental: Definir tiempos de retención para cada tipo de documento y automatizar el proceso de archivo o eliminación según las políticas de retención.
- Automatización de flujos de trabajo documentales: Integrar la gestión documental con los flujos de trabajo de la Contraloría para mejorar la eficiencia en el manejo de archivos y reducir el tiempo de acceso a la información.
- Capacitación en uso y administración del sistema: Realizar talleres de formación en el uso y la administración del sistema de gestión documental para el personal clave.

Responsables: Equipo del proceso de Tecnologías de Información y las Comunicaciones y el área de archivo.

Recursos:

- Financieros: Presupuesto para el software de gestión documental y digitalización.
- Humanos: Personal de archivo y de proceso de TI.
- Tecnológicos: Licencias y equipos de digitalización.

Proyecto 4: Capacitación y Desarrollo de Competencias en TI
Objetivo: Fortalecer las competencias tecnológicas del personal mediante programas de capacitación continua.

Actividades:

- Desarrollo de un programa de capacitación continua en TI: Cursos en análisis de datos, ciberseguridad, y gestión de información.
- Certificación del personal de TI: Incentivar la obtención de certificaciones en áreas clave.
- Evaluación de impacto de la capacitación: Medir mejoras en habilidades y competencias.
- Desarrollo de un programa de capacitación personalizada: Adaptar los cursos a las necesidades específicas de cada área, permitiendo al personal centrarse en las herramientas y prácticas más relevantes para su rol.
- Simulaciones y ejercicios prácticos en ciberseguridad: Implementar talleres prácticos sobre ciberseguridad, como simulaciones de phishing y ejercicios de respuesta a incidentes, para fortalecer las habilidades en situaciones reales.
- Acceso a plataformas de e-learning con certificaciones: Proveer acceso a plataformas como Coursera o Udacity para que el personal complete cursos con certificaciones en TI, ciberseguridad y análisis de datos.
- Evaluación post-capacitación y seguimientos periódicos: Realizar pruebas de conocimientos y encuestas de evaluación después de cada capacitación para medir el impacto y ajustar futuros programas de formación.

Responsables: Recursos Humanos y el área del proceso de Tecnologías de la Información y las Comunicaciones.

Recursos:

- Financieros: Presupuesto para cursos y certificaciones.
- Humanos: Formadores especializados.
- Tecnológicos: Plataformas de e-learning y materiales de capacitación.

Proyecto 5: Integración e Interoperabilidad con otras Entidades Públicas
Objetivo: Facilitar el intercambio de datos y la colaboración con otras entidades para optimizar el control fiscal y la transparencia.

Actividades:

- Establecimiento de estándares de interoperabilidad: Definir estándares y protocolos para la integración.
- Desarrollo de interfaces de intercambio de datos: Crear conexiones seguras con entidades gubernamentales.
- Monitoreo y ajuste continuo de la interoperabilidad: Evaluar la eficiencia de la integración y ajustar.
- Desarrollo de interfaces API para el intercambio de información: Crear APIs para conectar los sistemas de la Contraloría Distrital de Cartagena de Indias con otras entidades de forma segura, optimizando la interoperabilidad.
- Estandarización de formatos de datos: Definir formatos estándar (por ejemplo, JSON, XML) para los datos compartidos entre entidades, asegurando compatibilidad y facilidad de integración.
- Establecimiento de acuerdos de nivel de servicio (SLA): Negociar SLAs con otras entidades para asegurar tiempos de respuesta y calidad de servicio en el intercambio de datos.
- Pruebas de interoperabilidad y ajustes: Ejecutar pruebas de interoperabilidad con sistemas externos y ajustar cualquier incompatibilidad antes de la implementación total.

Responsables: proceso de Tecnologías de Información y las Comunicaciones en colaboración con entidades aliadas.

Recursos:

- Financieros: Presupuesto para desarrollo de interfaces y licencias.
- Humanos: Personal del proceso de TI y especialistas en integración de datos.
- Tecnológicos: Infraestructura y herramientas de integración.

Proyecto 6: Desarrollo de Aplicativos de Software In-House para Apoyo a las labores misionales

Objetivo: Desarrollar y optimizar aplicaciones de software internas (in-house) que permitan a la Contraloría Distrital de Cartagena de Indias gestionar de forma efectiva y en tiempo real los procesos de control fiscal, facilitando la trazabilidad de observaciones y hallazgos y la gestión de resoluciones.

Este proyecto responde a la necesidad de contar con herramientas personalizadas que se ajusten a los requisitos específicos de la Contraloría Distrital de Cartagena de Indias, permitiendo una mayor agilidad en los procesos y un control más preciso de las etapas involucradas en los procesos de auditoría y control fiscal. Las aplicaciones in-house incluyen:

1. Sistema de Información para la Gestión de Resoluciones: Facilita el registro, control, y seguimiento de resoluciones, asegurando que los datos estén actualizados y accesibles para el personal y la ciudadanía en todo momento.
2. Sistema de Información para la Trazabilidad de Observaciones y Hallazgos: Permite llevar un registro detallado de las observaciones y hallazgos desde su identificación en el proceso auditor hasta la culminación de su ciclo de vida en el juicio de responsabilidad fiscal. Esto ayuda a gestionar y monitorear el avance y cierre de cada hallazgo.

Actividades:

- Análisis de Requerimientos y Diseño del Sistema
  Levantamiento de requisitos con usuarios clave: Realizar reuniones con el equipo auditor y demás usuarios para definir las funcionalidades específicas que cada sistema necesita. Prototipado y diseño de interfaz de usuario (UI): Diseñar un prototipo interactivo de la interfaz, permitiendo a los usuarios visualizar la estructura y la lógica de los sistemas antes de la programación.
- Desarrollo y Optimización de Módulos Funcionales
  - Sistema de Gestión de Resoluciones:
    - Módulos para el registro, actualización y consulta de resoluciones.
    - Funcionalidades de control de versiones y generación de reportes de estado de las resoluciones.
  - Sistema de Trazabilidad de Observaciones/Hallazgos:
    - Registro de hallazgos desde su identificación inicial hasta su cierre.
    - Funcionalidad de generación de informes que resuman el estado de cada observación/hallazgo.
    - Implementación de un dashboard visual con indicadores que muestren el avance del ciclo de vida de los hallazgos.
- Pruebas y Validación
  Pruebas unitarias y funcionales: Realizar pruebas para validar cada funcionalidad del sistema, asegurando que cumpla con los requerimientos definidos.
  Pruebas de usuario final y ajustes: Implementar un periodo de prueba con usuarios finales para identificar mejoras y realizar ajustes antes del despliegue total.

- Capacitación y Soporte a Usuarios
  Capacitación al personal: Realizar talleres de capacitación para el personal encargado de usar y administrar los sistemas.
  Soporte técnico y documentación: Generar manuales de usuario y documentación técnica para asegurar el correcto uso y mantenimiento de los sistemas.
  Responsables: Equipo del proceso de TI
- Recursos Humanos: Desarrolladores de software especializados en backend y frontend. Analistas de sistemas para el levantamiento de requerimientos y pruebas de calidad. Personal de soporte para el mantenimiento de los aplicativos y la atención de incidencias.
- Recursos Financieros: Presupuesto para herramientas de desarrollo y licencias de software, como bases de datos y librerías de código.
  Fondos para capacitación en el uso de las aplicaciones y en nuevas tecnologías para el equipo de desarrollo.
- Recursos Tecnológicos: Infraestructura de desarrollo como Servidores o entornos en la nube para alojar los sistemas y realizar pruebas.
  Herramientas de desarrollo y gestión de proyectos: Plataformas como GitLab o Jira para el control de versiones y la organización del equipo de desarrollo.

INDICADORES DE DESEMPEÑO Y SEGUIMIENTO

Los indicadores de desempeño permiten evaluar el avance de cada proyecto y su contribución a los objetivos estratégicos. Estos indicadores se revisarán periódicamente para hacer ajustes y asegurar el cumplimiento de los plazos y resultados esperados.

Indicadores para la Renovación de Infraestructura Tecnológica y Optimización de Redes

- Porcentaje de renovación de equipos: Mide el avance en la adquisición y reemplazo de hardware, reflejado como el porcentaje de equipos renovados en relación con el total planificado.
  Meta: Renovar al menos el 60% de los equipos al finalizar el primer año.
- Tiempo de disponibilidad de red: Refleja la estabilidad de la red y la conectividad interna. Meta: Mantener una disponibilidad superior al 98% mensual.
- Reducción en tiempo de respuesta del sistema: Mide la mejora en el rendimiento de los sistemas tras la optimización de la infraestructura.
  Meta: Reducir el tiempo de respuesta en un 40% en comparación con la situación actual.

Indicadores para el Fortalecimiento de la Seguridad de la Información y Protección de Datos

- Número de incidentes de seguridad: Refleja la eficacia de las medidas de seguridad implementadas y la reducción en vulnerabilidades.
  Meta: Reducir los incidentes en un 80% en el primer año.
- Nivel de cumplimiento de la Política de Tratamiento de Datos Personales: Evalúa la adecuación de las políticas de manejo de datos según la legislación.

Meta: Cumplimiento del 100% para el segundo trimestre.

- Porcentaje de personal capacitado en seguridad: Mide el avance en la formación del personal sobre prácticas de seguridad y protección de datos.
  Meta: Capacitar al 100% del personal al final del segundo año.
- Tiempo de detección de incidentes
  Meta: Reducir el tiempo de detección de amenazas y ataques en un 30% en el primer año.
- Porcentaje de datos clasificados y asegurados
  Meta: Asegurar que el 100% de los datos críticos tengan controles específicos de acceso y cifrado.

Indicadores para el Sistema de Gestión Documental

- Porcentaje de documentos digitalizados: Mide el progreso en la digitalización y organización documental.
  Meta: Digitalizar al menos el 50% de los documentos en el primer año.
- Reducción en el tiempo de búsqueda de documentos: Evalúa la efectividad del sistema documental en optimizar el acceso a la información.
  Meta: Reducir el tiempo de búsqueda en un 50% en comparación con los métodos anteriores.
- Grado de uso del sistema: Refleja el nivel de adopción y uso por parte del personal. Meta: Asegurar un uso superior al 90% entre los usuarios potenciales al finalizar el segundo año.

Indicadores para Capacitación y Desarrollo de Competencias en TI

- Número de capacitaciones realizadas: Mide el avance en la implementación del programa de capacitación.
  Meta: Completar al menos cuatro capacitaciones anuales.
- Evaluación de habilidades adquiridas: Mide el impacto de las capacitaciones en las habilidades del personal, evaluado a través de encuestas de competencias.
  Meta: Lograr una mejora del 70% en la calificación de habilidades en temas de TI.
- Satisfacción del personal con la capacitación: Evalúa la percepción del personal sobre el valor y utilidad de las capacitaciones.
  Meta: Obtener una satisfacción superior al 85% en las evaluaciones de capacitación.

Indicadores para la Interoperabilidad con otras Entidades Públicas

- Número de sistemas interoperables: Mide el avance en la integración de sistemas con otras entidades.
  Meta: Integrar al menos tres sistemas clave en el primer año.
- Reducción en tiempo de acceso a información externa: Mide la eficiencia del intercambio de información.
  Meta: Reducir el tiempo de acceso en un 50% en comparación con los tiempos actuales.

- Grado de colaboración en proyectos conjuntos: Refleja el nivel de cooperación en iniciativas compartidas con otras entidades.
  Meta: Participar en al menos dos proyectos conjuntos durante el periodo del PETI.

Indicadores para el desarrollo de Aplicativos de Software In- House para Apoyo a las labores misionales

- Tiempos de procesamiento de resoluciones
  Meta: Reducir el tiempo promedio de gestión de resoluciones en un 40% en comparación con métodos manuales.
- Porcentaje de cumplimiento en el ciclo de vida de hallazgos
  Meta: Aumentar el cumplimiento del ciclo de vida de los hallazgos en un 50%, asegurando el cierre de hallazgos en el tiempo estipulado.
- Nivel de satisfacción del usuario
  Meta: Obtener una satisfacción mínima del 85% en encuestas a usuarios sobre la funcionalidad y eficiencia de los sistemas.
  Reducción en errores de trazabilidad
  Meta: Reducir en un 60% los errores en el seguimiento de hallazgos gracias a la automatización y estandarización de procesos.

CRONOGRAMA DE IMPLEMENTACIÓN

El cronograma de implementación organiza los proyectos en fases para asegurar un despliegue efectivo y secuencial de las iniciativas. Se estima una duración de dos años para la implementación completa del PETI, distribuyendo los proyectos estratégicos en trimestres para un monitoreo eficaz.

Año 1

Fase	Trimestre 1	Trimestre 2	Trimestre 3	Trimestre 4
Proyecto 1	Evaluación y adquisición de equipos	Optimización de redes internas	Implementación de servicios en la nube (parcial)	Ajuste y monitoreo de infraestructura
Proyecto 2	Desarrollo de políticas de seguridad	Instalación de herramientas de ciberseguridad	Capacitación en seguridad (50%)	Ajustes en medidas de seguridad
Proyecto 3	Selección de software de gestión documental	Inicio de digitalización documental	Continuación de digitalización documental	Capacitación en uso del sistema
Proyecto 4	Plan de capacitación en TI	Primera ronda de certificaciones	Evaluación de competencias	Capacitación en TI continua
Proyecto 5	Definición de estándares de interoperabilidad	Desarrollo de interfaces de intercambio	Integración con entidades públicas (parcial)	Monitoreo de integración
Proyecto 6	Levantamiento de requisitos y diseño de prototipos	Revisión de prototipos y aprobación final	Inicio de desarrollo del Sistema de Gestión de	Desarrollo del Sistema de Trazabilidad de Hallazgos de

			Resoluciones	

Año 2

Fase	Trimestre 1	Trimestre 2	Trimestre 3	Trimestre 4
Proyecto 1	Continuación en la renovación de Equipos	Mantenimiento y actualización de red	Implementación total de servicios en la nube	Evaluación y ajustes finales
Proyecto 2	Revisión de política de seguridad	Segunda ronda de capacitación en seguridad	Auditoría de seguridad interna	Revisión de medidas y ajuste
Proyecto 3	Revisión del sistema documental	Completar digitalización documental	Optimización en el uso del sistema	Evaluación y mejoras finales
Proyecto 4	Segunda ronda de certificaciones	Capacitación avanzada en TI	Evaluación de impacto de capacitación	Revisión y plan de formación anual
Proyecto 5	Integración con sistemas adicionales	Proyecto conjunto con entidades	Monitoreo de eficiencia en intercambio de datos	Evaluación de interoperabilidad
Proyecto 6	Pruebas unitarias y funcionales	Pruebas de usuario y ajustes	Capacitación al personal en los sistemas desarrollados	Despliegue completo y soporte inicial

ASIGNACIÓN DE RECURSOS

Para garantizar la implementación exitosa del PETI, es esencial contar con una asignación clara y suficiente de recursos. Estos recursos incluyen el personal involucrado, el presupuesto estimado y las herramientas tecnológicas necesarias.

Recursos Humanos

Cada proyecto requiere de equipos específicos para su ejecución y seguimiento. La asignación de roles y responsabilidades es la siguiente:

- Equipo del proceso de TI: Encargado de la implementación técnica de los proyectos. Esto incluye la renovación de infraestructura, la implementación de sistemas de seguridad, y la configuración de sistemas interoperables.
- Talento Humano: Responsable de coordinar los programas de capacitación y sensibilización para el personal.
- Consultores Externos: Especialistas en áreas específicas como ciberseguridad, integración de sistemas y gestión documental. Estos consultores apoyarán los proyectos en los cuales se requieran conocimientos especializados no disponibles en el equipo interno.
- Auditores de TI: Profesionales encargados de realizar auditorías de seguridad y evaluar la conformidad con las políticas de seguridad de la información.

Recursos Financieros

El presupuesto estimado se asigna en función de las necesidades de cada proyecto, considerando tanto los costos iniciales como los gastos de mantenimiento y

actualización.

Recursos Tecnológicos
Para cada proyecto, se identifican las herramientas tecnológicas necesarias para su correcta implementación:

- Hardware y Dispositivos de Red: Renovación de servidores, estaciones de trabajo, y dispositivos de conectividad para asegurar la estabilidad de la red.
- Software de Seguridad: Herramientas de ciberseguridad como firewalls, sistemas de detección de intrusiones, y autenticación multifactor.
- Plataforma de Gestión Documental: Solución para el almacenamiento y organización de documentos, con características de búsqueda avanzada y seguridad de acceso.
- Plataformas de e-Learning: Recursos para facilitar la capacitación continua en temas de TI y seguridad.
- Herramientas de Interoperabilidad: Software y protocolos que permitan la integración con sistemas de otras entidades.

GESTIÓN DE RIESGOS

La gestión de riesgos es fundamental para anticipar posibles obstáculos y prepararse para afrontarlos de manera proactiva. A continuación, se presentan los riesgos principales asociados con la implementación del PETI y las estrategias de mitigación para cada uno.

Identificación de Riesgos

- Riesgo de insuficiencia presupuestaria:
  Descripción: El presupuesto asignado puede resultar insuficiente debido a gastos imprevistos o cambios en los costos del mercado.
  Impacto: Alto.
  Probabilidad: Media.
- Riesgo de resistencia al cambio por parte del personal:
  Descripción: Los empleados pueden mostrar resistencia a adoptar nuevas tecnologías y procesos debido a la falta de familiaridad o preocupación por el cambio.
  Impacto: Alto.
  Probabilidad: Alta.
- Riesgo de problemas de seguridad de la información:
  Descripción: Posible ocurrencia de brechas de seguridad o ciberataques que comprometan la información institucional.
  Impacto: Muy alto.
  Probabilidad: Media.
- Riesgo de dependencia de proveedores externos:
  Descripción: Dependencia de terceros para la implementación de ciertos proyectos, lo que puede provocar retrasos o problemas de calidad en las entregas.
  Impacto: Medio.
  Probabilidad: Media.
- Riesgo de problemas en la interoperabilidad con otras entidades:
  Descripción: Obstáculos técnicos o normativos que dificulten la integración con los sistemas de otras entidades públicas.
  Impacto: Alto.

Probabilidad: Media.

Estrategias de Mitigación
Acciones de mitigación para el riesgo de insuficiencia presupuestaria:

- Realizar un análisis de costos detallado y gestionar un fondo de contingencia del 10-15% del presupuesto inicial.
- Priorizar los proyectos según su impacto y buscar fuentes de financiamiento adicionales si es necesario.

Acciones de mitigación para el riesgo de resistencia al cambio por parte del personal:

- Implementar un plan de gestión del cambio que incluya sesiones de sensibilización y capacitación.
- Crear incentivos para el personal que adopte rápidamente los cambios y realizar encuestas de retroalimentación para ajustar el enfoque de adopción.

Acciones de mitigación para el riesgo de problemas de seguridad de la información:

- Fortalecer la infraestructura de seguridad mediante la instalación de herramientas avanzadas de ciberseguridad.
- Realizar auditorías de seguridad periódicas y entrenar al personal en prácticas de seguridad para minimizar vulnerabilidades.

Acciones de mitigación para el riesgo de dependencia de proveedores externos:

- Contratar proveedores con buena reputación y antecedentes comprobados en el cumplimiento de plazos.
- Incluir cláusulas de penalización en los contratos para asegurar el cumplimiento de entregas, así como planes de contingencia con proveedores alternativos.

Acciones de mitigación para el riesgo de problemas en la interoperabilidad con otras entidades:

- Establecer un equipo de trabajo dedicado a la interoperabilidad que trabaje en conjunto con representantes de otras entidades.
- Desarrollar protocolos y estándares de integración claros y evaluar previamente la compatibilidad tecnológica antes de iniciar los procesos de integración.

PLAN DE GESTIÓN DEL CAMBIO

Un Plan de Gestión del Cambio es esencial para asegurar que el personal de la Contraloría Distrital de Cartagena de Indias se adapte exitosamente a las nuevas tecnologías y procesos implementados en el PETI. Este plan tiene como objetivo minimizar la resistencia al cambio, promover la adopción de nuevas herramientas y facilitar la transición a los sistemas y procesos optimizados.

Objetivos del Plan de Gestión del Cambio
Objetivo General: Facilitar la adopción de nuevas tecnologías y procesos en la Contraloría Distrital de Cartagena de Indias, asegurando que el personal esté capacitado y motivado para integrar estas herramientas en su trabajo diario.

Objetivos Específicos:

- Reducir la resistencia al cambio mediante estrategias de comunicación y sensibilización.
- Capacitar al personal en el uso de nuevas aplicaciones, sistemas de información y herramientas de ciberseguridad.
- Asegurar que el cambio sea sostenible en el tiempo, integrando mecanismos de soporte y seguimiento.
- Crear una cultura de mejora continua, en la que los empleados valoren la innovación y el desarrollo tecnológico como parte esencial de su labor.

Análisis de Impacto del Cambio
Antes de implementar cualquier cambio, es crucial identificar qué áreas y procesos de la Contraloría se verán más afectados. Este análisis de impacto permite entender los desafíos específicos y diseñar estrategias de intervención adecuadas.

Actividades:

- Identificación de Procesos Afectados: Crear una lista de los procesos que cambiarán debido al PETI, como la gestión documental, la trazabilidad de hallazgos y el acceso a sistemas de auditoría.
- Mapeo de Impacto en el Personal: Identificar los roles y equipos que serán más afectados. Clasificar el personal en niveles según el grado de cambio que experimentarán (alto, medio, bajo).
- Evaluación de Competencias Actuales: Realizar una evaluación inicial de las competencias tecnológicas del personal para identificar brechas que deban ser cubiertas a través de la capacitación.

ESTRATEGIA DE COMUNICACIÓN
Una comunicación clara y frecuente es clave para reducir la incertidumbre y ayudar al personal a comprender la importancia del cambio. La estrategia de comunicación debe adaptarse a las distintas fases del proyecto.

Acciones:

- Comunicación Inicial del Cambio:
  - Organizar una reunión de lanzamiento con todo el personal para presentar el PETI, sus objetivos y beneficios.
  - Enviar un boletín digital que explique cómo el cambio impactará de manera positiva en la Contraloría Distrital de Cartagena de Indias.
- Actualizaciones Periódicas:

- Enviar correos informativos y realizar reuniones mensuales para actualizar al personal sobre los avances del PETI.
- Implementar una intranet o tablero de anuncios donde se publiquen noticias, preguntas frecuentes, y actualizaciones de proyectos.

- Feedback y Escucha Activa:
  - Organizar sesiones de preguntas y respuestas con los equipos más afectados.
  - Establecer un canal de comunicación directa (como un correo o chat de soporte) donde los empleados puedan expresar inquietudes y recibir respuestas rápidas.
- Enfoque en Beneficios para el Personal:
  Resaltar los beneficios concretos que el personal obtendrá con las nuevas herramientas (mejoras en la eficiencia, reducción de tareas repetitivas, mayor seguridad en sus actividades diarias).

Formación y Capacitación
La capacitación es un pilar fundamental para garantizar que el personal se sienta cómodo y competente al utilizar las nuevas tecnologías. Este plan debe adaptarse a las necesidades específicas de cada equipo y estar alineado con los cambios introducidos en el PETI.

- Fases de Capacitación:
  - Fase Inicial de Sensibilización:
    - Realizar talleres introductorios donde se expliquen los conceptos básicos de las nuevas tecnologías.
    - Enfatizar la importancia de la ciberseguridad y el manejo seguro de la información.
  - Capacitación Técnica por Proyecto:
    - Sistema de Gestión Documental: Capacitar al personal de archivo y administrativo en el uso de las herramientas de digitalización y organización de documentos.
    - Sistema de Trazabilidad de Observaciones/Hallazgos: Entrenar a los auditores y supervisores en el uso de dashboards, reportes y funcionalidades de trazabilidad.
    - Sistema de Gestión de Resoluciones: Formar al equipo de administración en el manejo del sistema, con módulos específicos para cada rol.
  - Capacitación Continua y Seguimiento:
    - Establecer un programa de formación continua en el que se impartan capacitaciones cada semestre para reforzar conocimientos y actualizar al personal en nuevas funciones.
    - Implementar un sistema de evaluación post-capacitación para medir la efectividad de la formación y hacer ajustes.
- Herramientas de Capacitación:
  - Simuladores de Procesos: Crear simulaciones de procesos para que el personal practique en un entorno seguro.

- Cursos en línea: Utilizar plataformas de e-learning donde los empleados puedan acceder a cursos y videos de capacitación.
- Manuales y Guías de Usuario: Elaborar manuales detallados de uso de cada sistema, así como videos tutoriales que faciliten el aprendizaje autodirigido.

Estrategias de Motivación y Reconocimiento

Para fomentar la adopción tecnológica, es útil implementar un sistema de motivación y reconocimiento. Esto puede ayudar a que el personal perciba el cambio como un proceso positivo.

Estrategias:

- Incentivos por Adopción Temprana: Ofrecer reconocimientos a los primeros empleados que demuestren dominio en los nuevos sistemas y procesos, como certificados o bonificaciones.
- Programa de Embajadores del Cambio: Seleccionar empleados voluntarios que sirvan como embajadores del cambio, motivando a sus compañeros y promoviendo una actitud positiva frente a la tecnología.
- Reconocimientos Públicos: Destacar los logros de los equipos que implementen exitosamente los cambios y adopten nuevas herramientas.

Monitoreo y Evaluación del Proceso de Cambio

Es fundamental establecer mecanismos de monitoreo para evaluar el progreso del cambio, identificar áreas problemáticas y ajustar el plan según sea necesario. El monitoreo puede hacerse en varias etapas.

- Indicadores de Evaluación:
  - Índice de Adopción Tecnológica: Medir el porcentaje de personal que utiliza activamente las nuevas herramientas.
  - Nivel de Satisfacción del Usuario: Realizar encuestas periódicas para recoger retroalimentación sobre la experiencia de los usuarios con las nuevas tecnologías.
  - Progreso en Competencias Tecnológicas: Evaluar el avance de las competencias tecnológicas mediante evaluaciones de conocimiento y práctica post- capacitación.
- Mecanismos de Seguimiento:
  - Revisiones Trimestrales de Avance: Reuniones con los responsables de cada área para evaluar el progreso del cambio y hacer ajustes.
  - Reporte semestral de Adopción: Un informe semestral que compile los indicadores de adopción, satisfacción y competencia, permitiendo a la alta dirección visualizar el progreso del cambio.
  - Feedback Continuo: Mantener un canal abierto para que los empleados expresen sus inquietudes y necesidades, adaptando la gestión del cambio a sus comentarios.

Soporte y Asistencia Continuos

Un soporte técnico y de usuario eficaz es crucial para acompañar al personal durante la transición y asegurar la continuidad en el uso de los nuevos sistemas.

- Estructura de Soporte:
  - Equipo de Soporte Especializado: Designar un equipo de soporte interno que esté disponible para resolver incidencias y dudas en el uso de las nuevas tecnologías.
  - Plataforma de Ticketing: Implementar un sistema de ticketing (como Zendesk o Freshdesk) para gestionar las solicitudes de soporte y hacer seguimiento a su resolución.
  - Soporte en Tiempo Real: Ofrecer opciones de soporte en tiempo real, como un chat o número de atención directa, para responder preguntas inmediatas.
- Materiales de Apoyo:
  - FAQs y Recursos de Autoayuda: Crear una base de conocimientos en la intranet con preguntas frecuentes, guías de usuario y videotutoriales.
  - Asistencia Post-Lanzamiento: Mantener el equipo de soporte activo por un periodo de tiempo extendido (tres a seis meses) después del lanzamiento de los sistemas.

Evaluación de Resultados y Retroalimentación Final

La última etapa del Plan de Gestión del Cambio implica la evaluación de los resultados y la recopilación de retroalimentación final para hacer ajustes en futuras implementaciones.

Acciones de Cierre:

- Encuesta de Retroalimentación Final: Realizar una encuesta final para evaluar la percepción del personal sobre el proceso de cambio, recogiendo comentarios sobre los aspectos que pueden mejorarse en futuras implementaciones.
- Informe de Resultados: Elaborar un informe que resuma los logros alcanzados, los obstáculos enfrentados y las lecciones aprendidas, proporcionando una guía para mejorar futuros proyectos de cambio.
- Reunión de Cierre: Organizar una reunión de cierre con todo el personal para agradecer su colaboración, compartir los resultados del cambio y reforzar la cultura de mejora continua.

PLAN DE CONTINUIDAD DEL NEGOCIO (BCP) Y RECUPERACIÓN ANTE DESASTRES (DRP)

Un Plan de Continuidad del Negocio (BCP) y un Plan de Recuperación ante Desastres (DRP) son componentes esenciales para garantizar que la Contraloría Distrital de Cartagena de Indias pueda mantener sus operaciones críticas y proteger la integridad de sus datos ante eventos adversos, como desastres naturales, fallos tecnológicos o ciberataques. Este plan permite que la organización pueda responder rápida y eficientemente a incidentes graves, asegurando la disponibilidad de los sistemas esenciales.

Objetivos del BCP y DRP

Objetivo General: Asegurar que la Contraloría Distrital de Cartagena de Indias pueda continuar sus operaciones críticas y restablecer los sistemas de TI en caso de interrupciones importantes, minimizando el impacto en la gestión y en la prestación de servicios.

Objetivos Específicos:

- Identificar y priorizar los sistemas y procesos críticos de la Contraloría Distrital de Cartagena de Indias.
- Definir protocolos de respuesta para distintos escenarios de desastres y fallos.
- Establecer tiempos de recuperación y objetivos de disponibilidad para cada sistema.
- Capacitar al personal en los procedimientos de respuesta ante incidentes y desastres.
- Revisar y mejorar continuamente el BCP y DRP para asegurar su efectividad ante nuevos riesgos.

Análisis de Impacto en el Negocio (BIA)
El Análisis de Impacto en el Negocio (BIA) es una evaluación exhaustiva que identifica las funciones críticas y calcula los efectos potenciales de una interrupción. Esta evaluación permite asignar prioridades y recursos para la recuperación de los sistemas más importantes.

Pasos del BIA:

- Identificación de Procesos Críticos: Listar las operaciones clave de la Contraloría Distrital de Cartagena de Indias (p. ej., auditoría, trazabilidad de hallazgos, gestión de resoluciones, Responsabilidad fiscal).
- Evaluación de Impacto por Proceso: Calcular el impacto financiero, reputacional y operativo de una interrupción en cada proceso.
- Definición de Tiempos de Recuperación (RTO/RPO):
  - o Objetivo de Tiempo de Recuperación (RTO): Determinar el tiempo máximo en el que cada proceso debe reanudarse tras una interrupción.
  - o Objetivo de Punto de Recuperación (RPO): Establecer la cantidad de datos que se puede permitir perder, definiendo la frecuencia de respaldos.
- Priorización de Procesos y Sistemas: Clasificar los procesos y sistemas según su nivel de criticidad para garantizar una recuperación secuencial y efectiva.

Estrategias de Respaldo y Recuperación
Contar con estrategias de respaldo sólidas y procedimientos de recuperación es fundamental para proteger los datos y garantizar la continuidad de los servicios.

Estrategias de Respaldo:

- Backups en la Nube: Configurar copias de seguridad automáticas en un entorno seguro de la nube, para garantizar la disponibilidad de los datos fuera del sitio físico.
- Backup Local con Redundancia: Mantener copias de seguridad locales en servidores redundantes ubicados en diferentes áreas de la Contraloría Distrital de Cartagena de Indias.

- Frecuencia de Respaldo: Establecer una política de respaldo diario para datos críticos y semanal para datos menos críticos, según los RPO establecidos en el BIA.
- Pruebas de Integridad de Respaldo: Implementar pruebas periódicas de restauración para asegurar que los respaldos se realicen correctamente y que los datos sean recuperables en caso de fallo.

Procedimientos de Recuperación:

- Plan de Recuperación por Escenarios:
  - Ciberataque: En caso de un ataque de ransomware, tener un plan para aislar los sistemas infectados, notificar al personal clave y activar la restauración de los respaldos más recientes.
  - Fallo Tecnológico Crítico: Establecer procedimientos para redirigir las operaciones a servidores de respaldo.
  - Desastre Natural: Activar el DRP con respaldo en la nube para permitir el acceso a los sistemas críticos desde ubicaciones remotas.
- Prioridad de Recuperación de Sistemas: Basado en el BIA, definir el orden de restauración de sistemas (p. ej., primero los sistemas de trazabilidad de hallazgos y auditoría, luego los sistemas administrativos).

Plan de Respuesta Inmediata ante Incidentes
Un plan de respuesta inmediata es clave para reducir el impacto del incidente desde el primer momento. Este plan debe especificar acciones concretas y responsables.

Acciones Inmediatas:

- Activación del Equipo de Respuesta ante Incidentes: Establecer un equipo de respuesta integrado por personal del proceso de TI, líderes de áreas críticas y el equipo de seguridad, encargado de tomar decisiones rápidas.
- Notificación y Escalamiento: Definir un protocolo de notificación para informar al personal clave y, si es necesario, a entidades externas (proveedores de servicios, reguladores).
- Contención Inicial: En caso de un ciberataque o falla crítica, tomar acciones de contención para evitar la propagación del problema (por ejemplo, desconectar temporalmente ciertos sistemas de la red).
- Evaluación de Daños: Realizar una evaluación inicial para determinar la gravedad del incidente y tomar decisiones sobre la activación del BCP o DRP.

Roles y Responsabilidades:

- Equipo de TI: Responsable de implementar medidas de contención y gestionar la recuperación técnica de los sistemas.
- Líderes de Áreas Críticas: Coordinar con el equipo del proceso de TI para restablecer los procesos en función de las prioridades definidas.

- Equipo de Comunicación: Gestionar la comunicación con el personal y, en caso necesario, con el público para brindar
información clara sobre el estado de los sistemas y las medidas de recuperación.

Plan de Continuidad del Negocio (BCP)
El BCP define los procedimientos para mantener las operaciones de la Contraloría Distrital de Cartagena de Indias en caso de interrupciones. Incluye procedimientos específicos para cada proceso clave.

Elementos del BCP:

- Procedimientos de Trabajo Alternativos: Documentar cómo realizar tareas críticas manualmente o con recursos limitados si los sistemas no están disponibles temporalmente.
- Puestos de Trabajo Remotos: Establecer estaciones de trabajo secundarias (p. ej., VPN y computadoras portátiles) para que el personal clave pueda continuar trabajando desde ubicaciones remotas.
- Planes de Comunicación en Emergencias: Crear un plan para mantener a todo el personal informado sobre el estado del incidente y las acciones de recuperación en curso.
- Pruebas Periódicas del BCP: Realizar simulacros de continuidad al menos una vez al año para evaluar la efectividad de los procedimientos y mejorar las áreas de debilidad detectadas.

Plan de Recuperación ante Desastres (DRP)
El DRP se enfoca en restablecer los sistemas de TI y minimizar el tiempo de inactividad después de un desastre. Este plan incluye procedimientos de restauración específicos para cada sistema crítico y define los pasos para volver a un estado de normalidad.

Pasos del DRP:

- Recuperación de Infraestructura: Restablecer servidores, redes y estaciones de trabajo según el orden de prioridad definido.
- Restauración de Datos: Restaurar los datos desde los respaldos más recientes, siguiendo los objetivos de RTO y RPO para minimizar la pérdida de información.
- Verificación de Integridad y Pruebas Post-Recuperación: Validar que los sistemas recuperados funcionan correctamente y que los datos están íntegros. Realizar pruebas de operación en los sistemas críticos antes de la reanudación total.
- Evaluación Post-Incidente y Lecciones Aprendidas: Al finalizar la recuperación, realizar una revisión del proceso y documentar las lecciones aprendidas para mejorar el DRP en el futuro.

Capacitación y Concientización del Personal
Un elemento clave del BCP y DRP es la capacitación y concientización del personal, asegurando que todos sepan cómo actuar en caso de emergencia.

Actividades de Capacitación:

- Capacitación Inicial: Realizar sesiones de capacitación para el personal en los protocolos de respuesta, incluyendo simulacros de emergencias y entrenamiento en el uso de respaldos y herramientas de contingencia.
- Talleres de Simulacro: Ejercicios de simulacro con escenarios de desastres tecnológicos y naturales, donde el personal simule el uso del BCP y DRP en tiempo real.
- Programas de Concientización Continua: Programar sesiones de actualización cada seis meses para mantener a todo el personal informado sobre los procedimientos de respuesta y cualquier cambio en el BCP o DRP.

Evaluación y Mejora Continua del BCP y DRP
La revisión y mejora del BCP y DRP son esenciales para asegurar que el plan se mantenga actualizado y efectivo.

Actividades de Mejora:

- Revisión Semestral: Realizar una revisión cada seis meses para actualizar los procedimientos de respaldo, RTO y RPO, y ajustar los sistemas y prioridades según las necesidades actuales de la Contraloría Distrital de Cartagena de Indias.
- Auditorías Externas: Contratar auditorías externas para evaluar la efectividad del BCP y DRP, identificando áreas de mejora y validando el cumplimiento con normativas de continuidad y recuperación.
- Informe de Lecciones Aprendidas: Documentar todas las observaciones, ajustes y aprendizajes tras simulacros y eventos reales, incorporándolos en la revisión anual del plan.

ESTRATEGIA DE INNOVACIÓN Y ADOPCIÓN DE NUEVAS TECNOLOGÍAS

La Estrategia de Innovación y Adopción de Nuevas Tecnologías es esencial para que la Contraloría Distrital de Cartagena de Indias se mantenga actualizada en un entorno tecnológico en constante cambio, optimizando procesos y mejorando la eficiencia de las labores de auditoría, control y trazabilidad. Esta estrategia debe promover una cultura de innovación, exploración y adaptación rápida, asegurando que las tecnologías emergentes puedan aplicarse de manera efectiva para fortalecer los objetivos institucionales.

Objetivos de la Estrategia de Innovación y Adopción de Nuevas Tecnologías
Objetivo General: Establecer un marco para la identificación, evaluación e implementación de tecnologías innovadoras que optimicen los procesos misionales de la Contraloría Distrital de Cartagena de Indias, asegurando su competitividad y eficiencia.

bjetivos Específicos:

- Identificar tecnologías emergentes con el potencial de mejorar la auditoría, la gestión documental y la trazabilidad de hallazgos y resoluciones.
- Implementar pilotos de prueba y pruebas de concepto (PoC) para evaluar la aplicabilidad de nuevas tecnologías.
- Crear una cultura de innovación que involucre al personal en la exploración y adopción de soluciones tecnológicas.
- Formar al personal en nuevas competencias tecnológicas necesarias para operar herramientas emergentes.
- Asegurar una evaluación continua de las tecnologías adoptadas para medir su impacto y efectividad en el cumplimiento de la misión de la Contraloría Distrital de Cartagena de Indias.

Análisis de Tecnologías Emergentes
La estrategia debe empezar con un análisis sistemático de las tendencias tecnológicas y su posible impacto en la Contraloría Distrital de Cartagena de Indias. Este análisis incluye la identificación de tecnologías que tengan aplicaciones directas o indirectas en el sector público y de control fiscal.

Tecnologías Clave:

- Inteligencia Artificial (IA) y Aprendizaje Automático (ML): IA y ML pueden mejorar los procesos de auditoría al analizar grandes volúmenes de datos, detectar patrones de riesgo y realizar análisis predictivos para identificar posibles anomalías.
- Big Data y Análisis Avanzado de Datos: El análisis avanzado permite manejar y analizar grandes cantidades de datos financieros y operativos, facilitando la auditoría, la identificación de irregularidades y la generación de reportes de desempeño.
- Blockchain: Aplicable para asegurar la trazabilidad y la integridad de los registros de auditoría, resoluciones y hallazgos, proporcionando una infraestructura de datos inalterable y transparente.
- Computación en la Nube: Permite una gestión de datos flexible, accesible y con alta disponibilidad, facilitando el trabajo remoto, el respaldo de información y la escalabilidad de los servicios de TI.
- Robotic Process Automation (RPA): Ideal para automatizar tareas repetitivas en la auditoría y en la gestión de resoluciones, como la actualización de registros y la generación de reportes, lo que permite liberar al personal para tareas de mayor valor.

Proceso de Evaluación de Tecnologías:

- Escaneo del Entorno Tecnológico: Monitorear periódicamente informes, investigaciones y tendencias en tecnología aplicable al sector público y de control fiscal.
- Evaluación de Viabilidad: Analizar la viabilidad de cada tecnología en términos de presupuesto, infraestructura actual y compatibilidad con los sistemas existentes.

- Análisis de Beneficio-Costo: Evaluar el costo de adopción e implementación de cada tecnología, en comparación con los beneficios que puede ofrecer en términos de eficiencia, tiempo y ahorro en costos operativos.
- Priorización de Tecnologías: Clasificar las tecnologías en función de su aplicabilidad y el valor que pueden aportar a las áreas misionales de la Contraloría.

Implementación de Proyectos Piloto y Pruebas de Concepto (PoC)
Los proyectos piloto y las pruebas de concepto son esenciales para validar el uso de nuevas tecnologías en un entorno controlado antes de implementarlas a gran escala.

Proceso de Implementación de Pilotos:

- Selección de Proyectos Piloto: Identificar proyectos específicos que permitan evaluar la funcionalidad de la tecnología y su impacto en procesos clave, como auditoría, responsabilidad fiscal o gestión documental.
- Definición de Metas y KPIs del Piloto: Establecer objetivos claros para cada piloto, con indicadores clave de rendimiento (KPIs) que midan su efectividad (por ejemplo, reducción del tiempo de auditoría o mejora en la trazabilidad de hallazgos).
- Asignación de Recursos: Asignar un equipo de proyecto y definir el presupuesto, herramientas y apoyo técnico necesario para ejecutar el piloto.
- Evaluación de Resultados: Realizar una revisión exhaustiva de los resultados obtenidos y de los KPIs. Documentar los aprendizajes y definir si la tecnología es apta para una implementación completa o si requiere ajustes.

Desarrollo de Competencias en Innovación y Nuevas Tecnologías
Para que la adopción de nuevas tecnologías sea exitosa, el personal debe estar capacitado y preparado para utilizarlas de manera efectiva. Esto requiere un plan de desarrollo de competencias.

Estrategia de Capacitación:

- Identificación de Necesidades de Capacitación: Realizar un análisis de brechas en competencias tecnológicas en el personal actual para determinar qué habilidades son necesarias.
- Programas de Capacitación Especializada: Diseñar cursos en temas específicos, como análisis de datos, manejo de sistemas en la nube, ciberseguridad avanzada, y RPA, para preparar al personal en las tecnologías que se adoptarán.
- Certificación en Nuevas Tecnologías: Incentivar al personal a obtener certificaciones relevantes, como certificaciones en análisis de datos, administración de sistemas en la nube, o IA aplicada.
- Entrenamiento en Innovación y Cultura de Cambio: Realizar talleres que promuevan una mentalidad innovadora, con técnicas de design thinking y mejora continua, motivando al personal a participar activamente en el desarrollo de soluciones tecnológicas.

Modalidades de Capacitación:

- Plataformas de E-Learning: Proveer acceso a plataformas como Coursera, Udemy o edX para capacitación autodirigida en temas específicos.
- Workshops y Seminarios Internos: Organizar seminarios con expertos en tecnologías emergentes y talleres prácticos de manejo de herramientas tecnológicas.
- Mentoría y Rotación de Roles: Implementar un sistema de mentoría donde empleados con habilidades avanzadas puedan guiar a sus colegas, y fomentar la rotación de roles en proyectos tecnológicos para ampliar la experiencia del personal.

Cultura de Innovación y Mejora Continua
Fomentar una cultura de innovación es fundamental para que el personal de la Contraloría Distrital de Cartagena de Indias adopte una actitud proactiva hacia la exploración y el uso de nuevas tecnologías.

Estrategias de Fomento de Cultura Innovadora:

- Creación de un Equipo de Innovación Tecnológica: Formar un grupo especializado que se encargue de investigar, proponer y pilotear nuevas tecnologías, y que actúe como un laboratorio interno de innovación.
- Programa de Ideas Abiertas: Establecer un canal donde los empleados puedan sugerir mejoras tecnológicas, proponiendo soluciones a problemas operativos.
- Reconocimiento e Incentivos: Implementar un sistema de reconocimiento para aquellos empleados que participen en proyectos de innovación o presenten ideas que optimicen los procesos institucionales.
- Sesiones de Innovación: Realizar reuniones semestrales de innovación donde se presenten tendencias tecnológicas, estudios de caso y avances en los pilotos de tecnología, fomentando el diálogo y la colaboración.

Evaluación y Medición del Impacto de Nuevas Tecnologías
Es crucial establecer mecanismos de evaluación para medir el impacto de las tecnologías implementadas, asegurando que realmente contribuyan a la misión de la Contraloría.

Indicadores de Evaluación:

- ROI de Tecnología: Calcular el retorno de inversión de cada tecnología en función del ahorro de costos, el aumento en la eficiencia y los beneficios operativos.
- Impacto en la Eficiencia de Procesos: Medir la reducción en tiempos de auditoría, mejora en la trazabilidad de hallazgos, procesos de responsabilidad fiscal y otros indicadores de desempeño.
- Satisfacción del Usuario Final: Realizar encuestas periódicas al personal que utiliza las nuevas tecnologías para evaluar su percepción sobre la facilidad de uso y los beneficios obtenidos.
- Mejora en Seguridad y Cumplimiento: Verificar que las tecnologías implementadas hayan fortalecido la seguridad de los datos y mejorado el cumplimiento de regulaciones, con métricas de reducción de incidentes de seguridad.

Revisión y Ajustes:

- Evaluación Trimestral de Tecnologías: Realizar revisiones semestrales de las tecnologías implementadas para identificar áreas de mejora o ajustes necesarios.
- Informe Anual de Innovación: Elaborar un informe anual que resuma los proyectos de innovación, los resultados de cada piloto y las recomendaciones para futuras implementaciones.
- Plan de Actualización Tecnológica: Establecer un calendario de actualización y modernización de tecnologías, asegurando que las herramientas adoptadas se mantengan vigentes y efectivas.

Plan de Financiamiento para Innovación
La estrategia debe incluir un plan de financiamiento que asegure los recursos necesarios para el desarrollo y la adopción de nuevas tecnologías.

Fuentes de Financiamiento:

- Presupuesto Interno de Innovación: Asignar una parte del presupuesto anual para proyectos de innovación tecnológica.
- Convocatorias y Subsidios: Participar en convocatorias y programas de financiamiento para innovación tecnológica en el sector público.
- Alianzas Público-Privadas: Establecer acuerdos de colaboración con el sector privado u otras entidades del sector público para recibir apoyo en investigación y desarrollo de tecnologías aplicadas al control fiscal.

PLAN DE GESTIÓN DE LA CALIDAD

El Plan de Gestión de la Calidad asegura que las implementaciones del PETI cumplan con altos estándares de efectividad y satisfacción, alineándose con los objetivos de la Contraloría Distrital de Cartagena de Indias y ofreciendo un marco para la mejora continua. Este plan establece procesos para evaluar, controlar y mejorar la calidad de cada proyecto, servicio o sistema tecnológico, con el fin de garantizar una operación óptima y la satisfacción del personal y los usuarios.

Objetivos del Plan de Gestión de la Calidad
Objetivo General: Garantizar que todos los proyectos y sistemas implementados en el marco del PETI cumplan con los estándares de calidad establecidos y contribuyan efectivamente a los objetivos de la Contraloría Distrital de Cartagena de Indias, mejorando la eficiencia y optimizando el uso de recursos.

Objetivos Específicos:

- Definir y monitorear estándares de calidad para cada proyecto del PETI.
- Implementar mecanismos de control de calidad en todas las fases de desarrollo e implementación de sistemas.

- Establecer una cultura de calidad y mejora continua en el área de TI y en los procesos de la Contraloría Distrital de Cartagena de Indias.
- Involucrar a los usuarios en la evaluación de calidad para asegurar que los sistemas cumplan con sus necesidades y expectativas.
- Asegurar el cumplimiento de normativas y estándares nacionales e internacionales de calidad en TI.

Establecimiento de Estándares de Calidad
Definir los estándares de calidad es el primer paso para asegurar que todos los proyectos y procesos de TI cumplan con los niveles de eficiencia, seguridad y funcionalidad requeridos.

Principales Estándares de Calidad:

- ISO 9001: Asegura la implementación de un sistema de gestión de la calidad (SGC) que promueva la mejora continua en los procesos de TI.
- ISO/IEC 20000: Estándar para la gestión de servicios de TI que asegura la calidad en la provisión y el soporte de servicios tecnológicos.
- ISO/IEC 27001: Estándar en gestión de seguridad de la información, aplicable a los procesos y sistemas para proteger la confidencialidad e integridad de los datos.
- NORMAS ITIL (Information Technology Infrastructure Library): Proporciona mejores prácticas en la gestión de servicios de TI, cubriendo desde el diseño hasta la operación y mejora continua.

Criterios de Calidad por Área:

- Eficiencia Operativa: Medición del rendimiento de los sistemas en términos de tiempo de respuesta y velocidad de procesamiento.
- Disponibilidad: Determinación del porcentaje de tiempo en el que los sistemas están operativos y disponibles para los usuarios.
- Seguridad: Evaluación de la protección de los datos y la resistencia de los sistemas frente a ciberataques y brechas de seguridad.
- Satisfacción del Usuario: Medición de la satisfacción de los usuarios finales en cuanto a la facilidad de uso, funcionalidad y soporte recibido.

Procesos de Control de Calidad
El control de calidad debe implementarse en cada fase de los proyectos de TI para identificar y corregir problemas desde el inicio. Estos controles incluyen revisiones periódicas y la aplicación de pruebas específicas.

Actividades de Control de Calidad:

- Revisión de Requerimientos: Asegurar que los requerimientos iniciales de cada proyecto estén claramente definidos y aprobados, alineándose con los objetivos y necesidades de la Contraloría Distrital de Cartagena de Indias.

- Pruebas de Desarrollo: Realizar pruebas de calidad en las primeras etapas del desarrollo de sistemas, incluyendo pruebas unitarias, funcionales y de integración para detectar fallos o inconsistencias.
- Pruebas de Usuario (UAT): Involucrar a usuarios clave en pruebas de aceptación para validar que el sistema cumple con los requisitos y es adecuado para el uso cotidiano.
- Auditorías Internas de Calidad: Programar auditorías periódicas para revisar el cumplimiento de los estándares de calidad y detectar áreas de mejora.

Herramientas de Control de Calidad:

- Herramientas de Testing Automático: Emplear software de pruebas como Selenium o JMeter para realizar pruebas automáticas que garanticen la funcionalidad y el rendimiento de los sistemas.
- Tableros de Control de Calidad (Dashboards): Implementar tableros visuales para monitorear indicadores clave de calidad en tiempo real y facilitar la toma de decisiones.
- Métricas de Análisis de Código: Utilizar herramientas de análisis de código (p. ej., SonarQube) para revisar la calidad del código y asegurar que cumpla con estándares de buenas prácticas de desarrollo.

Indicadores de Calidad y Métricas de Desempeño
Para medir la calidad de los proyectos, es importante definir indicadores clave de desempeño (KPIs) que permitan monitorear el avance y detectar desviaciones.

Indicadores de Calidad:

- Cumplimiento de Requerimientos: Porcentaje de requerimientos completados en cada sistema.
- Tiempo de Respuesta del Sistema: Tiempo promedio de respuesta de los sistemas en operaciones críticas, comparado con los objetivos de rendimiento establecidos.
- Porcentaje de Disponibilidad: Medición del tiempo total de disponibilidad de cada sistema, con un objetivo mínimo del 99% en sistemas críticos.
- Número de Incidentes y Fallos: Frecuencia y gravedad de incidentes técnicos reportados, evaluados para cada sistema.
- Nivel de Satisfacción del Usuario: Resultado promedio de encuestas de satisfacción realizadas a usuarios, con un objetivo mínimo de satisfacción del 85%.

Herramientas de Monitoreo de KPIs:

- Software de Monitoreo en Tiempo Real: Implementar herramientas como Zabbix o Nagios para monitorear el rendimiento de los sistemas en tiempo real.
- Paneles de KPI Personalizados: Desarrollar dashboards específicos donde se presenten los KPIs de calidad, facilitando el seguimiento y la toma de decisiones informadas.

Proceso de Mejora Continua

El plan de gestión de la calidad debe incorporar un ciclo de mejora continua, basado en el modelo PDCA (Plan-Do-Check-Act). Este ciclo permite revisar y optimizar los procesos de TI para adaptarse a cambios en los requerimientos y asegurar una mejora constante.

Fases del Ciclo PDCA:

- Planificar (Plan): Definir objetivos de calidad y estrategias de implementación para cada proyecto, alineándolos con los objetivos estratégicos de la Contraloría.
- Hacer (Do): Implementar los planes de calidad y realizar las actividades de desarrollo o mejora según lo planeado.
- Verificar (Check): Evaluar los resultados obtenidos con los KPIs y compararlos con los objetivos de calidad. Detectar errores y áreas de mejora.
- Actuar (Act): Implementar ajustes y optimizaciones en los procesos, estandarizando las mejores prácticas e incorporando los aprendizajes en futuras implementaciones.

Estrategias para la Mejora Continua:

- Encuestas y Retroalimentación del Usuario: Realizar encuestas de satisfacción y recoger comentarios de los usuarios para identificar áreas de mejora y oportunidades de ajuste.
- Benchmarking de Calidad: Comparar los procesos y resultados con contralorías y organizaciones similares para identificar prácticas exitosas que puedan implementarse.
- Revisión semestral de Procesos: Realizar reuniones semestrales para revisar los resultados de los indicadores de calidad y ajustar las estrategias conforme sea necesario.

Auditoría de Calidad y Cumplimiento

Las auditorías de calidad permiten evaluar el cumplimiento de los estándares y detectar posibles desviaciones, además de asegurar que los procesos cumplen con las normativas internas y externas aplicables.

Tipos de Auditorías:

- Auditorías Internas: Realizadas por el equipo de calidad o un equipo de control interno para evaluar la conformidad de los sistemas y procesos con los estándares de calidad de la Contraloría Distrital de Cartagena de Indias.
- Auditorías Externas: Contratación de una entidad externa especializada en auditorías de TI que evalúe el cumplimiento de los estándares ISO y las normativas aplicables.
- Auditorías de Satisfacción del Usuario: Evaluación del uso de los sistemas por parte de los usuarios finales, midiendo su nivel de satisfacción y usabilidad, y verificando si los sistemas cumplen con los requisitos funcionales y de accesibilidad.

Frecuencia y Seguimiento:

- Auditorías Semestrales: Realizar auditorías internas cada seis meses para

monitorear el cumplimiento y detectar necesidades de ajuste.

- Informes de Auditoría: Documentar los resultados de cada auditoría, especificando hallazgos, recomendaciones y plazos para la implementación de mejoras.

Capacitación en Gestión de Calidad
Para asegurar la implementación efectiva del plan de gestión de calidad, el personal del proceso de TI debe estar capacitado en estándares de calidad y mejores prácticas de control.

Estrategias de Capacitación:

- Capacitación en Normas de Calidad (ISO, ITIL): Ofrecer formación específica en normas de calidad aplicables al ámbito de TI, como ISO 9001, ISO 20000 e ITIL.
- Talleres de Mejora Continua: Organizar talleres prácticos en los que el personal de TI y los líderes de proyectos puedan trabajar en la mejora de procesos y en el análisis de KPIs.
- Certificación de Personal Clave: Incentivar la obtención de certificaciones en gestión de calidad, como ISO 9001 Lead Auditor o ITIL Foundation, para asegurar que el equipo cuenta con los conocimientos necesarios.

Evaluación y Reporte de Resultados de Calidad
Evaluar y reportar los resultados de calidad permite a la dirección de la Contraloría conocer el estado de los proyectos y tomar decisiones informadas para mejorar los procesos.

Elementos del Reporte de Calidad:

- Resumen de KPIs de Calidad: Presentación de los principales indicadores de calidad de cada proyecto, con análisis de los resultados y comparación con los objetivos.
- Hallazgos de Auditoría y Evaluación: Documentación de los hallazgos de auditoría y de las áreas de mejora detectadas.
- Planes de Acción para la Mejora: Especificación de acciones correctivas o preventivas que deben implementarse para mejorar los resultados de calidad.

Frecuencia de Reportes:

- Reportes Semestrales: Reportes semestrales con indicadores de calidad, auditorías realizadas y áreas de mejora propuestas.
- Informe Anual de Calidad: Resumen anual que incluya el rendimiento en calidad durante el año, los cambios implementados y recomendaciones para el año siguiente.

MAPA DE RIESGOS TECNOLÓGICOS DETALLADO

El Mapa de Riesgos Tecnológicos Detallado es una herramienta clave para identificar, evaluar y mitigar los riesgos asociados con el uso de tecnologías en la Contraloría Distrital de Cartagena de Indias. Este mapa no solo ayuda a minimizar el impacto de posibles incidentes en los sistemas de TI y en las operaciones críticas, sino que también asegura que la organización esté preparada para gestionar los riesgos de forma proactiva.

A continuación, se desglosa cada componente del mapa de riesgos, incluyendo las categorías, la metodología de evaluación, estrategias de mitigación y un sistema de seguimiento.

Objetivos del Mapa de Riesgos Tecnológicos

Objetivo General: Identificar, clasificar y gestionar los riesgos tecnológicos que puedan afectar la integridad, disponibilidad y confidencialidad de los sistemas de información y procesos críticos de la Contraloría Distrital de Cartagena de Indias.

Objetivos Específicos:

- Identificar los riesgos tecnológicos más relevantes y clasificar su nivel de criticidad.
- Establecer un plan de acción para la mitigación, monitoreo y respuesta ante riesgos.
- Minimizar el impacto de incidentes tecnológicos en la operación diaria de la Contraloría.
- Asegurar la preparación del equipo del proceso de TI y del personal clave para actuar ante potenciales incidentes.
- Evaluar y actualizar el mapa de riesgos periódicamente para adaptarse a cambios tecnológicos y nuevos desafíos.

Categorías de Riesgos Tecnológicos

Para estructurar el mapa de riesgos, es útil clasificar los riesgos en distintas categorías, de modo que se facilite la asignación de medidas de mitigación específicas.

Principales Categorías de Riesgos:

- Riesgos de Seguridad de la Información: Incluyen ataques cibernéticos (p. ej., ransomware, phishing), accesos no autorizados, y pérdidas de datos críticos. Estos riesgos afectan la confidencialidad y la integridad de los datos.
- Riesgos de Operatividad y Continuidad: Asociados con interrupciones en los sistemas críticos, fallas en servidores, problemas de conectividad y falta de disponibilidad de sistemas esenciales para la operación.
- Riesgos de Cumplimiento Normativo: Incluyen el incumplimiento de leyes y normativas de TI, como protección de datos personales, estándares de seguridad y regulaciones específicas de auditoría.
- Riesgos de Infraestructura y Hardware: Cubren el deterioro o fallos de hardware, problemas de almacenamiento o fallas de redes que pueden afectar la continuidad de los sistemas de TI.
- Riesgos de Software y Desarrollo: Incluyen errores en el software, problemas en el desarrollo de aplicaciones y mal funcionamiento de sistemas que podrían comprometer la eficiencia operativa.
- Riesgos Humanos y de Capacitación: Relacionados con el error humano, falta de capacitación, manejo inapropiado de datos y otras acciones que puedan afectar la seguridad y funcionalidad de los sistemas.

Evaluación de Riesgos

La evaluación de riesgos implica medir el nivel de impacto y la probabilidad de cada riesgo, para determinar su criticidad. Este proceso permite establecer un sistema de priorización para la implementación de medidas de mitigación.

Proceso de Evaluación de Riesgos:

- Identificación de Amenazas: Analizar las amenazas que pueden afectar cada categoría de riesgo (p. ej., ciberataques, fallas técnicas, errores humanos).
- Análisis de Probabilidad: Evaluar la probabilidad de que cada riesgo ocurra, utilizando una escala que varía desde baja hasta alta.
- Evaluación de Impacto: Estimar el impacto de cada riesgo en las operaciones de la Contraloría, utilizando una escala que va de leve a crítico, considerando factores como el tiempo de inactividad y la pérdida de datos.
- Matriz de Riesgos: Crear una matriz de riesgos que ubique cada riesgo en función de su probabilidad e impacto, clasificándolos en riesgos bajos, moderados y críticos.

Clasificación en la Matriz de Riesgos

Riesgo	Descripción	Categoría	Probabilidad	Impacto	Nivel de Riesgo	Estrategia de mitigación	Responsable
Ataque de Ransomware	Bloqueo de acceso a sistemas y datos mediante cifrado, con solicitud de pago para liberación.	Seguridad de la Información	Alta	Crítico	Muy Alto	- Implementar copias de seguridad diarias - Autenticación multifactor (MFA) - Capacitación en reconocimiento de amenazas	Equipo de TI y Seguridad
Acceso no autorizado a datos sensibles	Acceso de personas no autorizadas a datos confidenciales o sensibles.	Seguridad de la Información	Alta	Crítico	Muy Alto	- Configuración de roles y permisos - Auditoría regular de accesos - Implementación de MFA para accesos privilegiados	Administrador de Seguridad

Fallo en servidor de auditoría	Interrupción del sistema de auditoría por fallos técnicos en el servidor principal.	Operatividad y Continuidad	Media	Alto	Alto	- Implementar servidores redundantes - Mantenimiento preventivo - Monitoreo en tiempo real de rendimiento	Equipo de Infraestructura
Incumplimiento de normativas de protección de datos	Incumplimiento de leyes y regulaciones sobre protección de datos personales y confidenciales.	Cumplimiento Normativo	Media	Alto	Alto	- Capacitación continua en normativas de protección de datos - Auditorías semestrales de cumplimiento - Revisiones periódicas de políticas de privacidad	Departamento Legal y TI
Error en el desarrollo aplicaciones	Problemas de funcionalidad en aplicaciones internas debido a errores de	Software Desarrollo	Baja	Moderado	Medio	- Pruebas de usuario (UAT) y pruebas unitarias	Equipo de Desarrollo

	desarrollo o pruebas incompletas.					- Revisiones de calidad de código - Capacitación en buenas prácticas de desarrollo	
Fallas de hardware (servidores o redes)	Pérdida de funcionalidad debido al deterioro o fallo de equipos físicos.	Infraestructura y Hardware	Media	Alto	Alto	- Implementación de redundancia de hardware - Contrato de soporte técnico - Mantenimiento preventivo regular	Equipo de Infraestructura
Ataques de phishing y malware	Suplantación de identidad y propagación de malware a través de correos electrónicos y enlaces maliciosos.	Seguridad de la Información	Alta	Alto	Muy Alto	- Capacitación en ciberseguridad y reconocimiento de phishing - Filtrosde correo y software antivirus - Sistema de detección y respuesta de amenazas (IDS/IPS)	Equipo de Seguridad
Interrupción de conectividad de red	Pérdida de conexión a internet o red interna, afectando el acceso a sistemas críticos.	Operatividad y Continuidad	Media	Alto	Alto	- Contratar ISP redundante - Balanceo de carga y failover de red - Monitoreo de red en tiempo real	Equipo de Redes y Conectividad

Falta de capacitación del personal en nuevas tecnologías	Desconocimiento o mala utilización de los nuevos sistemas por falta de entrenamiento adecuado.	Humano y Capacitación	Media	Moderado	Medio	- Plan de capacitación continua - Programa de formación en nuevas tecnologías - Capacitación en seguridad y buenas prácticas de TI	Recursos Humanos y TI
Perdida de datos en aplicaciones críticas	Pérdida de datos por errores en los sistemas o falta de copias de seguridad.	Seguridad de la Información	Baja	Critico	Alto	- Realizar copias de seguridad automáticas y fuera del sitio - Implementar pruebas de recuperación periódicas - Uso de bases de datos replicadas	Administrador de Sistemas
Brechas en la interoperabilidad con otras entidades	Dificultad en el intercambio de datos y procesos con otros sistemas del gobierno.	Infraestructura y Operatividad	Media	Moderado	Medio	- Implementación de estándares de interoperabilidad - Desarrollo de APIs seguras - Pruebas de compatibilidad con sistemas externos	Equipo de Integración
Fallo en el sistema de trazabilidad de hallazgos	Interrupción del sistema de gestión de observaci	Operatividad y Continuidad	Baja	Alto	Medio	- Copias de seguridad regulares y recuperación rápida - Plan de	Administrador de Sistemas

	ones y hallazgos en el proceso auditor.					contingencia manual para registro de hallazgos	

						- Capacitación del personal clave	
Error humano en manejo de datos sensibles	Divulgación accidental o incorrecta de datos sensibles debido a errores humanos.	Humano y Capacitación	Media	Alto	Alto	- Capacitación en manejo seguro de información - Políticas de manejo y acceso seguro de datos - Supervisión en procesos de alta sensibilidad	Equipo de Seguridad y Recursos Humanos
Desactualización de software y sistemas	Riesgo de vulnerabilidades y pérdida de funcionalidad por no contar con versiones actualizadas.	Software y Desarrollo	Alta	Moderado	Alto	- Establecimiento de un calendario de actualizaciones - Contratos de soporte y actualización de software - Pruebas de funcionalidad posterior a cada actualización	Equipo de Desarrollo y Seguridad

Estrategias de Mitigación por Categoría de Riesgo
Cada categoría de riesgo requiere estrategias de mitigación específicas para minimizar la probabilidad de ocurrencia y el impacto de los riesgos asociados.

Mitigación de Riesgos de Seguridad de la Información:

- Implementación de Firewalls y Sistemas de Detección de Intrusos (IDS/IPS): Configurar firewalls avanzados y sistemas de detección de intrusos para bloquear accesos no autorizados y detectar actividad sospechosa.
- Autenticación Multifactor (MFA): Exigir autenticación multifactor para todos los accesos a sistemas críticos.
- Copia de Seguridad y Plan de Recuperación ante Desastres: Realizar copias de seguridad diarias y pruebas de restauración periódicas para proteger y recuperar

los datos ante un ataque de ransomware.

- Capacitación en Ciberseguridad: Entrenar al personal en el reconocimiento de amenazas comunes, como el phishing y el malware.

Mitigación de Riesgos de Operatividad y Continuidad:

- Infraestructura Redundante y Balanceo de Carga: Implementar servidores redundantes y balanceo de carga para asegurar la continuidad de sistemas críticos en caso de fallas.
- Monitoreo de Sistemas en Tiempo Real: Utilizar herramientas de monitoreo para detectar problemas de rendimiento en los sistemas y actuar de manera preventiva.
- Plan de Continuidad del Negocio (BCP): Asegurar que el BCP esté activo y que incluya procedimientos claros para mantener la operatividad en caso de interrupciones.

Mitigación de Riesgos de Cumplimiento Normativo:

- Revisión y Actualización de Políticas: Mantener actualizadas las políticas de TI para alinearlas con las normativas nacionales e internacionales en protección de datos y seguridad de la información.

- Auditorías de Cumplimiento: Realizar auditorías de cumplimiento al menos dos veces al año para verificar el cumplimiento de normativas y estándares.
- Capacitación en Normativas de Protección de Datos: Asegurar que el personal esté capacitado en la Ley de Protección de Datos y en las normativas aplicables a la Contraloría Distrital de Cartagena de Indias.

Mitigación de Riesgos de Infraestructura y Hardware:

- Mantenimiento Preventivo: Realizar un mantenimiento preventivo periódico de los servidores, estaciones de trabajo y dispositivos de red para asegurar su funcionamiento óptimo.
- Gestión de Inventario de Hardware: Llevar un inventario detallado de todos los dispositivos de hardware, identificando aquellos que requieran reemplazo o actualización.
- Contrato de Soporte Técnico: Establecer contratos de soporte con proveedores de hardware para asegurar reparaciones rápidas y repuestos en caso de fallas críticas.

Mitigación de Riesgos de Software y Desarrollo:

- Pruebas de Calidad de Código: Implementar pruebas de calidad de código y realizar auditorías de desarrollo para detectar errores y mejorar la funcionalidad de los sistemas.
- Gestión de Actualizaciones: Crear un calendario de actualizaciones para los sistemas críticos, asegurando que se implementen las últimas versiones de seguridad.
- Plan de Pruebas de Usuario Final: Involucrar a los usuarios en pruebas de aceptación de software (UAT) para garantizar que las aplicaciones cumplen con los requisitos y funcionan correctamente.

Mitigación de Riesgos Humanos y de Capacitación:

- Capacitación en Gestión de Sistemas: Entrenar al personal en el uso de los sistemas de TI y en prácticas seguras para el manejo de datos sensibles.
- Protocolos de Manejo Seguro de Información: Implementar políticas claras para el manejo seguro de la información, previniendo errores humanos.
- Estrategia de Gestión de Cambio: Integrar la gestión de cambio en cada implementación de tecnología para reducir la resistencia y minimizar los errores operativos.

Plan de Monitoreo y Seguimiento de Riesgos

Para asegurar que los riesgos se gestionen adecuadamente, es necesario implementar un sistema de monitoreo y seguimiento continuo. Esto implica realizar revisiones periódicas y mantener registros actualizados de cada riesgo.

Actividades de Monitoreo:

- Revisión Trimestral de Riesgos: Revisar trimestralmente el estado de cada riesgo y evaluar la efectividad de las medidas de mitigación aplicadas.

- Actualización del Mapa de Riesgos: Ajustar el mapa de riesgos para reflejar cambios en la infraestructura tecnológica, actualizaciones en normativas o nuevos riesgos emergentes.
- Reuniones de Seguimiento con Equipos Clave: Realizar reuniones periódicas con los responsables de TI y de seguridad para evaluar y discutir el estado de los riesgos y cualquier incidencia reciente.

Herramientas de Monitoreo:

- Dashboard de Riesgos: Implementar un tablero visual donde se visualicen los riesgos activos, su nivel de criticidad y su estado actual.
- Sistema de Reportes de Incidentes: Utilizar una herramienta de registro de incidentes (p. ej., Jira Service Desk) para documentar y monitorear cualquier incidente o riesgo identificado.
- Indicadores de Control de Riesgos (KRIs): Establecer indicadores de control de riesgos que muestren el nivel de exposición a riesgos, como el número de incidentes de seguridad o el tiempo promedio de resolución de fallas.

Revisión y Actualización del Mapa de Riesgos
El mapa de riesgos debe actualizarse continuamente para reflejar cambios en el entorno tecnológico, nuevas amenazas y el estado de los controles implementados.

Frecuencia de Revisión:

- Revisión Semestral Completa: Realizar una revisión completa del mapa de riesgos cada seis meses para incorporar cambios en la tecnología, normativas o resultados de auditorías.
- Revisión Ad-Hoc tras Incidentes: Actualizar el mapa de riesgos inmediatamente después de incidentes significativos para evaluar si el riesgo necesita ser reclasificado o si se deben fortalecer las medidas de mitigación.

Informe de Riesgos Anual:

- Informe de Riesgos: Elaborar un informe anual que detalle los riesgos gestionados, los incidentes registrados, los resultados de las auditorías de riesgo y las recomendaciones para el año siguiente.
- Revisión y Retroalimentación del Equipo: Compartir el informe con los equipos de TI, seguridad y alta dirección para evaluar las estrategias de mitigación implementadas y ajustar las prioridades.

ESTRATEGIA DE EVALUACIÓN DE IMPACTO SOCIAL

La Estrategia de Evaluación de Impacto Social es fundamental para que la Contraloría Distrital de Cartagena de Indias pueda medir y demostrar cómo las mejoras tecnológicas y las iniciativas implementadas en el PETI benefician a los ciudadanos y fortalecen la transparencia, la eficiencia y la confianza en la gestión pública. Esta estrategia se enfoca en evaluar cómo las nuevas

herramientas y procesos afectan tanto a la ciudadanía como a la percepción de transparencia y responsabilidad de la Contraloría.

Objetivos de la Estrategia de Evaluación de Impacto Social
Objetivo General: Medir y demostrar el impacto positivo de las iniciativas tecnológicas en los ciudadanos y la transparencia en la gestión pública de la Contraloría Distrital de Cartagena de Indias, asegurando que estas mejoras contribuyan efectivamente a fortalecer la confianza pública y a fomentar una administración responsable.

Objetivos Específicos:

- Evaluar cómo las nuevas tecnologías mejoran la accesibilidad, eficiencia y transparencia en los servicios de la Contraloría Distrital de Cartagena de Indias.
- Identificar y medir indicadores de satisfacción ciudadana y percepción de transparencia en los procesos de control fiscal.
- Facilitar la rendición de cuentas a la ciudadanía y mejorar la comunicación sobre los avances en control fiscal.
- Promover una cultura de mejora continúa basada en los resultados de impacto social, ajustando estrategias y procesos conforme a las necesidades y expectativas de los ciudadanos.

Indicadores Clave de Impacto Social
Para medir el impacto social, se establecen indicadores específicos que reflejan el beneficio directo e indirecto de los cambios tecnológicos en los ciudadanos y en la percepción pública.

Indicadores Principales:

- Accesibilidad de la Información Pública:
- Cantidad de consultas ciudadanas: Número de accesos al portal de transparencia o a herramientas de información pública.
- Tasa de respuesta a solicitudes de información: Tiempo promedio de respuesta a las solicitudes ciudadanas.

Percepción de Transparencia:

- Nivel de confianza en la Contraloría: Medido mediante encuestas de opinión sobre la percepción de transparencia y responsabilidad en el uso de recursos públicos.
- Reducción en quejas por falta de transparencia: Cantidad de quejas ciudadanas relacionadas con la transparencia en los procesos de auditoría y gestión fiscal.

Eficiencia en la Atención Ciudadana:

- Tiempo promedio de resolución de consultas: Tiempo desde la recepción de una consulta hasta su resolución.
- Porcentaje de cumplimiento de los tiempos de atención: Proporción de consultas resueltas dentro del plazo estipulado.

Satisfacción Ciudadana:

- Encuestas de satisfacción: Nivel de satisfacción de los ciudadanos en la interacción con los servicios de la Contraloría Distrital de Cartagena de Indias, medido a través de encuestas.
- Frecuencia de interacción ciudadana: Número de interacciones o solicitudes realizadas por ciudadanos en un periodo determinado, indicando el nivel de involucramiento con los procesos de la Contraloría Distrital de Cartagena de Indias.

Indicadores Complementarios:

- Impacto en la eficiencia de procesos internos: Medir la eficiencia en los procesos de auditoría y control y cómo estos afectan la capacidad de respuesta a la ciudadanía.
- Uso de canales digitales: Evaluar el nivel de adopción y uso de canales digitales, como el portal web y redes sociales, para la consulta de información pública.

Metodología de Evaluación del Impacto Social
La metodología de evaluación incluye técnicas cuantitativas y cualitativas para captar tanto los resultados medibles como la percepción y satisfacción de los ciudadanos.

Fases del Proceso de Evaluación:

Recolección de Datos:

- Encuestas y Cuestionarios: Realizar encuestas periódicas dirigidas a los ciudadanos para evaluar la satisfacción, la percepción de transparencia y la accesibilidad a la información.
- Análisis de Interacciones en Línea: Monitorear las interacciones en la página web, redes sociales y plataformas de transparencia para medir el número de accesos y el tipo de información más consultada.
- Registro de Consultas y Quejas: Documentar consultas y quejas ciudadanas relacionadas con transparencia, atención y accesibilidad, clasificándolas para identificar áreas de mejora.

Análisis de Resultados:

- Evaluación de Indicadores: Revisar y analizar los datos recolectados sobre los indicadores de impacto social, comparándolos con los objetivos previamente establecidos.
- Análisis Comparativo: Comparar los resultados actuales con los datos de periodos anteriores para evaluar tendencias y mejoras a lo largo del tiempo.
- Interpretación de Resultados Cualitativos: Analizar los comentarios y opiniones ciudadanas para identificar la percepción general de la ciudadanía y las áreas en las que se requiere una mayor transparencia o mejor acceso a la información.

Reportes y Presentación de Resultados:

- Informe Trimestral de Impacto Social: Presentar un informe trimestral con los resultados obtenidos en cada indicador, destacando los logros, áreas de mejora y recomendaciones para ajustar estrategias.

- Infografías y Resúmenes para el Público: Elaborar resúmenes gráficos y accesibles que puedan compartirse en la página web y
  redes sociales, mostrando el impacto de las iniciativas de manera sencilla y transparente para la ciudadanía.

Estrategias de Participación Ciudadana y Transparencia
Para garantizar un impacto social positivo, es importante involucrar a los ciudadanos en el proceso de evaluación y hacer que el acceso a la información sea lo más abierto y sencillo posible.

Estrategias Clave:

- Sesiones de Diálogo Abierto: Realizar reuniones abiertas o foros virtuales donde los ciudadanos puedan expresar sus opiniones, sugerencias y necesidades directamente a los responsables de la Contraloría Distrital de Cartagena de Indias.
- Portal de Transparencia y Acceso a la Información: Asegurar que el portal de transparencia esté actualizado, sea fácil de navegar y permita el acceso a documentos y reportes de auditoría.
- Mecanismo de Retroalimentación Continua: Establecer un sistema de retroalimentación en el portal y redes sociales donde los ciudadanos puedan realizar comentarios y preguntas, asegurando respuestas oportunas.
- Campañas de Sensibilización: Promover campañas informativas sobre el uso de las nuevas herramientas y los derechos ciudadanos de acceso a la información y participación en los procesos de control fiscal.

Análisis y Mejora Continua Basada en Impacto Social
Para que la estrategia sea sostenible, se necesita un enfoque de mejora continúa basado en los resultados de la evaluación de impacto social. Esto garantiza que las iniciativas de TI se ajusten a las necesidades cambiantes de la ciudadanía y mejoren continuamente.

Actividades de Mejora Continua:

- Revisión Semestral de Estrategias: Evaluar los resultados de impacto social cada seis meses y ajustar las estrategias de acuerdo con los comentarios y necesidades de los ciudadanos.
- Actualización de Servicios y Herramientas: Basado en los resultados de satisfacción ciudadana, ajustar y mejorar las herramientas tecnológicas y los servicios de atención.
- Monitoreo de Nuevas Expectativas Sociales: Realizar encuestas de expectativas ciudadanas para entender mejor los cambios en las demandas de transparencia y accesibilidad y adaptar las estrategias conforme a estas expectativas.

Ejemplo de Proceso de Mejora:

- Identificación de Necesidades: Si la ciudadanía expresa dificultades para acceder a reportes específicos en el portal de transparencia, se deben identificar las áreas que requieren una mejora de acceso.

- Desarrollo de Soluciones: Implementar mejoras en la navegación del portal o simplificar la estructura de categorías para facilitar el acceso a la información.
- Reevaluación de Satisfacción: Tras implementar cambios, realizar una nueva encuesta de satisfacción para medir el éxito de la mejora.

Comunicación de Resultados y Transparencia Pública
Los resultados de la evaluación de impacto social deben ser comunicados a la ciudadanía de forma accesible y transparente. Esto no solo fortalece la confianza pública, sino que también permite a los ciudadanos ver el valor de las iniciativas tecnológicas.

Estrategias de Comunicación:

- Informe Anual de Impacto Social: Publicar un informe anual en la página web de la Contraloría Distrital de Cartagena de Indias que detalla el impacto de las iniciativas tecnológicas en términos de transparencia, eficiencia y satisfacción ciudadana.
- Boletines de Transparencia: Enviar boletines periódicos que informen sobre los resultados más relevantes de la evaluación de impacto social y los avances en los proyectos de TI.
- Infografías en Redes Sociales: Crear infografías que resuman los resultados clave y compartirlas en redes sociales para alcanzar a un público amplio de manera rápida y efectiva.
- Portal de Datos Abiertos: Establecer un portal de datos abiertos donde se publiquen datos relevantes sobre el desempeño de la Contraloría, permitiendo que los ciudadanos realicen sus propios análisis.

Plan de Financiamiento y Recursos para la Evaluación de Impacto Social
Para asegurar la implementación efectiva de la estrategia, es fundamental contar con un plan de financiamiento que cubra los recursos necesarios.

Recursos Clave:

- Presupuesto para Encuestas y Análisis: Financiamiento para contratar herramientas de encuestas, plataformas de análisis de datos y consultores especializados en impacto social.
- Equipo de Evaluación de Impacto Social: Designar un equipo interno que se encargue de la recolección de datos, análisis de resultados y generación de reportes.
- Tecnología para el Monitoreo de Interacciones: Invertir en herramientas de análisis de datos y monitoreo de interacciones ciudadanas en línea para captar y evaluar en tiempo real el impacto de las iniciativas de TI.

Estrategias de Financiamiento:

- Asignación Presupuestaria Anual: Establecer un presupuesto anual dedicado a la evaluación de impacto social y a las mejoras en transparencia.

- Convenios con Organismos de Transparencia: Colaborar con organizaciones de transparencia y responsabilidad pública para
  recibir asesoría y apoyo financiero en la implementación de iniciativas de acceso a la información.

ANÁLISIS DE IMPACTO AMBIENTAL DE LA TECNOLOGÍA

El Análisis de Impacto Ambiental de la Tecnología busca identificar y mitigar los efectos ambientales negativos asociados con el uso de tecnologías y prácticas de TI en la Contraloría Distrital de Cartagena de Indias. Este análisis permite evaluar aspectos como el consumo energético, la generación de residuos electrónicos y el uso de recursos naturales, promoviendo una gestión más sostenible de las tecnologías y minimizando el impacto ambiental.

Objetivos del Análisis de Impacto Ambiental de la Tecnología

Objetivo General: Evaluar y reducir el impacto ambiental derivado del uso de tecnologías en la Contraloría, promoviendo prácticas de TI sostenibles que minimicen el consumo de energía y la generación de residuos electrónicos.

Objetivos Específicos:

- Identificar las fuentes principales de impacto ambiental en el uso de tecnologías.
- Implementar prácticas de TI que optimicen el consumo energético y reduzcan la huella de carbono.
- Gestionar los residuos electrónicos de manera responsable, promoviendo el reciclaje y la reutilización de equipos.
- Fomentar una cultura de sostenibilidad en el área de TI y en la organización en general.
- Evaluar y mejorar continuamente las prácticas ambientales en TI.

Identificación de las Principales Fuentes de Impacto Ambiental

Para estructurar un plan efectivo de mitigación, es fundamental identificar las áreas de la infraestructura de TI que generan un mayor impacto ambiental.

Principales Fuentes de Impacto:

- Consumo de Energía en Centros de Datos y Equipos: Los centros de datos, servidores y dispositivos de computación son responsables de gran parte del consumo energético.
- Uso de Papel en Procesos Administrativos y de TI: Aunque la digitalización reduce el consumo de papel, ciertas áreas pueden continuar con prácticas que generan un alto uso de papel.
- Generación de Residuos Electrónicos: La renovación de equipos, como computadores, impresoras y servidores, genera residuos electrónicos que requieren una gestión adecuada.
- Emisiones de Carbono de los Equipos de TI: Las emisiones derivadas del uso de electricidad para mantener la infraestructura de TI y la energía consumida en el ciclo de vida de los dispositivos.

Análisis Inicial:

- Medición del Consumo de Energía: Realizar una evaluación energética de los dispositivos y equipos de la Contraloría Distrital de Cartagena de Indias para identificar los equipos con mayor consumo.
- Evaluación de Residuos Electrónicos Generados: Analizar la frecuencia de reemplazo de equipos, el volumen de residuos generados y los métodos de disposición actuales.
- Análisis de Ciclo de Vida de Equipos: Considerar el impacto ambiental de la adquisición, uso y disposición de cada equipo, determinando su huella de carbono total.

Estrategias para Reducir el Impacto Ambiental de las Tecnologías
Una vez identificadas las fuentes de impacto, se pueden implementar estrategias específicas para reducir el impacto ambiental de las actividades de TI en la Contraloría Distrital de Cartagena de Indias.

Estrategias para Reducir el Consumo Energético:

- Optimización de Centros de Datos:
  - Migrar servicios a la nube, cuando sea posible, para reducir el consumo de energía en la infraestructura local.
- Prácticas de Ahorro de Energía en Equipos:
  - Configurar políticas de ahorro de energía en computadoras y otros dispositivos, activando el modo de suspensión cuando no se están utilizando.
  - Incentivar el uso de equipos energéticamente eficientes y con certificaciones como Energy Star.
  - Implementar sensores de apagado automático para dispositivos electrónicos en áreas de poco uso.
- Uso de Energía Renovable:
  - Considerar fuentes de energía renovable, como paneles solares, para alimentar una parte de la infraestructura de TI.
  - Establecer un plan para evaluar proveedores de energía que ofrezcan opciones de energía renovable.

Estrategias para la Reducción de Residuos Electrónicos:

- Política de Extensión de la Vida Útil de Equipos:
  - Mantener y reparar equipos regularmente para prolongar su vida útil y reducir la necesidad de reemplazos.
  - Promover el reacondicionamiento y la reutilización de dispositivos en buen estado para otros fines dentro de la organización.
- Programa de Reciclaje y Disposición Responsable:
  - Establecer un convenio con empresas certificadas en reciclaje de residuos electrónicos para asegurar su correcta disposición.

- Donar equipos que aún funcionen pero que ya no sean necesarios en la Contraloría Distrital de Cartagena de Indias
  a instituciones educativas o benéficas, contribuyendo a una segunda vida útil.
- Crear estaciones de reciclaje de residuos electrónicos en las instalaciones para que el personal pueda disponer de pequeños dispositivos de forma adecuada.

Estrategias para la Reducción del Uso de Papel:

- Políticas de Oficina Sin Papel:
  - Promover la digitalización de documentos y archivos para reducir el uso de papel, almacenando información en sistemas digitales y de gestión documental.
  - Incentivar el uso de firmas electrónicas en procesos administrativos y de TI.
  - Limitar las impresiones a situaciones estrictamente necesarias, y fomentar el uso de impresión a doble cara.
- Capacitación en Prácticas de Oficina Ecológica:
  - Capacitar al personal sobre el uso eficiente del papel y la adopción de prácticas de oficina ecológicas.
  - Publicar recordatorios sobre prácticas de ahorro de papel, como imprimir solo cuando sea necesario y utilizar documentos digitales.

Indicadores de Impacto Ambiental y Métricas de Seguimiento
Definir indicadores clave permite medir y evaluar el impacto de cada acción ambiental y ajustar las estrategias según los resultados.

Indicadores Principales:

- Consumo Energético de Infraestructura de TI: Medición mensual del consumo energético de equipos, comparándolo con periodos anteriores.
- Cantidad de Residuos Electrónicos Generados: Volumen de residuos electrónicos generados anualmente, midiendo la cantidad reciclada, donada y desechada de manera responsable.
- Uso de Papel en Procesos de TI: Medición del consumo de papel mensual y reducción de impresiones, observando el cambio tras implementar prácticas de oficina sin papel.
- Huella de Carbono de la Infraestructura de TI: Cálculo anual de la huella de carbono generada por el consumo energético de equipos y la producción de residuos electrónicos.

Herramientas para el Monitoreo:

- Monitores de Consumo Energético: Instalar dispositivos de monitoreo de consumo energético en servidores y centros de datos para obtener datos precisos.
- Sistema de Inventario de Residuos: Implementar un sistema de inventario para rastrear la cantidad de residuos electrónicos generados y su método de disposición.
- Software de Gestión de Documentos: Implementar un sistema de gestión documental para monitorear el uso de documentos digitales y la reducción de

papel.

Estrategias de Sensibilización y Capacitación en Sostenibilidad

Involucrar al personal en la estrategia ambiental es esencial para fomentar una cultura de sostenibilidad en la Contraloría Distrital de Cartagena de Indias.

Actividades de Sensibilización:

- Campañas de Conciencia Ambiental: Realizar campañas internas de conciencia ambiental para educar al personal sobre el impacto de las tecnologías y prácticas sostenibles.
- Capacitación en TI Verde: Organizar sesiones de capacitación sobre prácticas de TI sostenible, como el uso adecuado de los equipos, el reciclaje de residuos y el ahorro de energía.
- Día del Medio Ambiente: Celebrar el Día del Medio Ambiente con actividades de reciclaje y charlas informativas sobre prácticas sostenibles en la oficina.

Incentivos para Prácticas Sostenibles:

- Reconocimientos a Prácticas Ecológicas: Reconocer a los equipos que adopten prácticas de ahorro energético y reciclaje con certificaciones o recompensas simbólicas.
- Programa de Embajadores Verdes: Designar embajadores de sostenibilidad en cada área para promover y liderar la adopción de prácticas ecológicas.

Evaluación Continua y Reportes de Impacto Ambiental

La evaluación continua permite medir el avance en la reducción del impacto ambiental y ajustar las estrategias en función de los resultados obtenidos.

Proceso de Evaluación:

- Revisión Trimestral de Indicadores Ambientales: Revisar los datos de consumo energético, residuos electrónicos y uso de papel cada trimestre para identificar áreas de mejora.
- Informe Anual de Sostenibilidad: Publicar un informe anual de sostenibilidad que incluya todos los indicadores de impacto ambiental, los logros alcanzados y las áreas de mejora.

Mejora Continua:

- Ajuste de Estrategias Basado en Resultados: Modificar las estrategias de acuerdo con los resultados del análisis ambiental y las recomendaciones de los equipos de TI y sostenibilidad.
- Retroalimentación del Personal: Recopilar comentarios del personal sobre las prácticas implementadas y sugerencias para mejorar la sostenibilidad en el área de TI.

Comunicación de Resultados y Transparencia Ambiental

Comunicar los resultados de la estrategia de sostenibilidad permite mejorar la imagen de la Contraloría y aumentar la confianza pública en sus prácticas responsables.

Estrategias de Comunicación:

- Portal de Transparencia Ambiental: Publicar los logros ambientales en el portal de transparencia, incluyendo datos sobre ahorro energético, reducción de residuos y mejora en la sostenibilidad.
- Boletines de Sostenibilidad: Enviar boletines internos y externos sobre los logros de la estrategia de impacto ambiental.
- Infografías en Redes Sociales: Crear infografías que resuman los principales resultados y compartirlas en redes sociales para que el público conozca el compromiso ambiental de la Contraloría.

Plan de Financiamiento para Iniciativas Ambientales
Para implementar efectivamente estas prácticas sostenibles, es importante contar con los recursos financieros adecuados.

Recursos Necesarios:

- Presupuesto para Energía Renovable y Equipos Eficientes: Asignación de recursos para la adquisición de equipos con eficiencia energética y la implementación de energías renovables en la infraestructura de TI.
- Inversión en Programas de Reciclaje: Financiamiento para programas de reciclaje y disposición adecuada de residuos electrónicos.
- Capacitación y Campañas de Sensibilización: Recursos para desarrollar campañas y capacitar al personal en sostenibilidad y prácticas de TI verde.

EVALUACIÓN Y REVISIÓN DEL PETI

La evaluación y revisión del PETI son fundamentales para garantizar su relevancia y efectividad a lo largo del tiempo. Este proceso permitirá a la Contraloría Distrital de Cartagena de Indias medir los resultados alcanzados y realizar ajustes en las estrategias según las necesidades cambiantes del entorno.

Evaluación del Desempeño
La evaluación se realizará de forma continua y se centrará en los siguientes aspectos:

- Monitoreo de Indicadores: Los indicadores de desempeño establecidos en el punto corresponiente se monitorearán periódicamente para evaluar el progreso hacia los objetivos. Esto incluye la recopilación de datos trimestrales sobre el avance de cada proyecto y su impacto en la organización.
- Revisión Semestral de Proyectos: Se llevarán a cabo reuniones semestrales para revisar el estado de cada proyecto, discutiendo los logros, desafíos y cualquier ajuste necesario en los planes de acción. Estas reuniones incluirán a todos los equipos responsables de la implementación de los proyectos.
- Auditorías Anuales: Realizar auditorías anuales que evalúen el cumplimiento de las políticas y procedimientos establecidos, así como la efectividad de las medidas de

seguridad implementadas. Esto ayudará a identificar áreas de mejora y a asegurar la transparencia en la gestión de recursos.

Revisión del PETI
La revisión del PETI se llevará a cabo anualmente y consistirá en:

- Actualización de Objetivos: Evaluar la pertinencia de los objetivos estratégicos en función de los cambios en la legislación, la tecnología y las necesidades institucionales. Si es necesario, se modificarán o añadirán objetivos para reflejar la realidad actual.
- Ajustes en el Cronograma y Recursos: Realizar un análisis de la ejecución de los proyectos, ajustando el cronograma y la asignación de recursos según los resultados obtenidos y las prioridades emergentes.
- Retroalimentación del Personal: Recoger la opinión y sugerencias del personal sobre la implementación del PETI a través de encuestas y grupos de discusión, lo que ayudará a identificar aspectos que podrían mejorarse y fomentar un ambiente de participación.
- Informe de Resultados: Elaborar un informe anual que resuma los resultados de la evaluación y revisión del PETI, incluyendo el progreso en los indicadores, lecciones aprendidas y recomendaciones para el futuro. Este informe se compartirá con todos los niveles de la organización para fomentar la transparencia y la rendición de cuentas.