PLAN DE MANTENIMIENTO DE SERVICIOS TECNOLÓGICOS

Bogotá D.C., 26 de enero de 2026

Contenido

1 INTRODUCCIÓN 3

2 ALCANCE DEL PLAN 3

3 OBJETIVO 4

4 OBJETIVOS ESPECÍFICOS 4

5 ESTRATEGIAS 4

6 PRODUCTOS 5

7 RESPONSABLES 5

8 PROYECTOS 6

1.1 Plan de Mantenimiento Preventivo 6

1.2 Plan de Mantenimiento Correctivo 6

1.3 Plan de Gestión de Activos Tecnológicos 6

1.4 Plan de Gestión de Riesgos Tecnológicos 7

1.5 Plan de Mantenimiento de Infraestructura Crítica 7

1.6 Plan de Ventanas de Mantenimiento 7

1.7 Plan de Evidencias y Documentación 7

1.8 Plan de Mejora Continua 8

9 ACCIONES 8

10 PLANES GENERALES DE COMPRAS QUE DESAGREGUEN LOS RECURSOS ASOCIADOS A TODAS LAS FUENTES DE FINANCIACIÓN 8

11 INDICADORES 9

12 CRONOGRAMA 10

13 MAPAS DE RIESGOS 10

1 INTRODUCCIÓN

El adecuado funcionamiento de la infraestructura tecnológica es fundamental para garantizar la continuidad operativa, la disponibilidad de la información y la prestación eficiente de los servicios institucionales. Con el incremento en la demanda de sistemas, aplicaciones y recursos tecnológicos, se hace indispensable establecer lineamientos que aseguren su mantenimiento preventivo y correctivo, así como su monitoreo permanente.

En este contexto, el **Plan de Mantenimiento de Servicios Tecnológicos 2026** se formula como una herramienta de gestión que permite organizar, programar y ejecutar las actividades necesarias para preservar en óptimas condiciones los equipos y componentes que soportan los sistemas de información de la entidad. Este plan contribuye a minimizar fallas, mitigar riesgos, fortalecer la seguridad tecnológica y garantizar la disponibilidad de los servicios críticos para el cumplimiento de la misión institucional.

El documento presenta las acciones, responsables, procedimientos y frecuencias definidas para el mantenimiento de los recursos tecnológicos, con el propósito de asegurar una operación estable, segura y alineada con los estándares técnicos exigidos.

2 ALCANCE DEL PLAN

Inicia con la definición del cronograma de mantenimiento preventivos lógicos y físicos de la infraestructura tecnológica que soporta los sistemas de información de la entidad y finaliza con la verificación exitosa de la funcionalidad de los equipos intervenidos en la ejecución del mantenimiento.

La programación de las fechas del mantenimiento a los equipos se planeará de acuerdo con las condiciones actuales de la entidad referente a los procesos contractuales, disponibilidad de proveedores expertos en la materia, recursos económicos y humanos, la criticidad de los servicios que soportan los dispositivos y el estado de estos.

Los activos tecnológicos que aplican para el cronograma de mantenimientos son:

- Equipos Servidores
- Equipos de Seguridad
- Equipos de Comunicaciones
- Equipos de Control de Acceso
- Equipos de UPS (UNINTERRUPTIBLE POWER SUPPLY) y Aires Acondicionados del Data Center
- Computadores de escritorio y Computadores portátiles
- Impresoras y Escáner

3 OBJETIVO

Definir un plan de mantenimiento para los equipos que hacen parte de la infraestructura tecnológica y soportan los sistemas de información de la entidad, con el propósito de garantizar la continuidad, disponibilidad y seguridad de los servicios tecnológicos.

4 OBJETIVOS ESPECÍFICOS

- Establecer estrategias de mantenimiento alineadas con las necesidades operativas y presupuestales
- Documentar resultados como diagnósticos, informes técnicos y actas de seguimiento, asegurando trazabilidad.
- Asignar responsables para ejecución, seguimiento y control del plan de mantenimiento, promoviendo coordinación entre áreas.
- Realizar la distribución presupuestal de forma eficiente, acorde con los proyectos de inversión y las fuentes de financiación.
- Definir actividades específicas preventivas, correctivas y de mejora que aseguren óptimo funcionamiento de los activos.
- Diseñar métricas que permitan evaluar cumplimiento, eficiencia operativa, disponibilidad de equipos y ejecución presupuestal.
- Construir un mapa de riesgos con causas, consecuencias y controles para asegurar un manejo preventivo y efectivo cuando se requiera.

5 ESTRATEGIAS

Teniendo en cuenta el objetivo estratégico del instituto de proteger y promover la salud de la población, mediante la gestión del riesgo asociada al consumo y uso de alimentos, medicamentos, dispositivos médicos y otros productos objeto de vigilancia sanitaria. Así como los objetivos estratégicos de la entidad:

- Contribuir a la mejora continua del estatus sanitario del país mediante el fortalecimiento de la inspección, vigilancia y control sanitario con enfoque de riesgo garantizando la protección de la salud de los colombianos y el reconocimiento nacional e internacional
- Prestar servicios con estándares de calidad para afianzar la confianza de la población
- Fortalecer la gestión del conocimiento, capacidades y competencias de los servidores públicos de la institución
- Contribuir a una Colombia legal y transparente mediante la implementación de acciones que mitiguen los efectos de la ilegalidad y la corrupción

Se plantean las siguientes estrategias para el mantenimiento de la infraestructura tecnológica:

- **Mantenimiento preventivo planificado** para proteger los activos críticos (servidor de Directorio Activo, servidor de bases de datos, comunicación y red).

- **Mantenimiento correctivo oportuno** basado en la criticidad del servicio afectado.
- **Monitoreo continuo y mantenimiento predictivo** en red, seguridad, datacenter y nube.
- **Gestión de parches y actualizaciones** de software, firmware y sistemas operativos.
- **Fortalecimiento de respaldos y continuidad del negocio**, incluyendo pruebas periódicas de restauración.
- **Gestión de proveedores**, SLAs y contratos de soporte.
- **Gestión de obsolescencia tecnológica** con planes de renovación para 2026.
- **Control de cambios** para evitar interrupciones en producción.
- **Documentación permanente** de cada actividad, incidente y hallazgo.
- **Ciclo de mejora continua**, basado en indicadores y análisis de riesgos.

6 PRODUCTOS

A continuación, se presentan los productos resultantes de la aplicación del presente plan, que se tienen en cuenta para la adquisición de bienes y servicios especializados

ITEM	ELEMENTOS	RESPONSABLE
1	Equipos servidores	Grupo de Soporte Tecnológico
2	Equipos de Seguridad	Grupo de Soporte Tecnológico
3	Equipos de Comunicaciones	Grupo de Soporte Tecnológico
5	Equipos de UPS yaires acondicionados del Centro de Datos	Grupo de Soporte Tecnológico
6	Computadoresde Escritorio ComputadoresPortátiles	Grupo de Soporte Tecnológico
7	Impresoras y Escáner	Grupo de Soporte Tecnológico
8	Bases de datos	Grupo de Gestión de Información
9	Aplicaciones	Grupo de Gestión de Información

7 RESPONSABLES

La Oficia de Tecnologías de la Información junto con sus coordinaciones y el Grupo de Soporte Tecnológico son los responsables del seguimiento a la ejecución de las actividades ejecutadas por contratistas, aliados o proveedores, así como la validación y ejecución de algunas actividades propias del personal de planta definidas en sus manuales de funciones.

8 PROYECTOS

Los mantenimientos, se planearán de acuerdo con las condiciones actuales de la entidad referente a los procesos contractuales de contratistas o proveedores expertos en la materia, la disponibilidad de recursos económicos y humanos, la criticidad de los servicios que soportan los dispositivos y el estado de estos.

Los informes y evidencias de mantenimientos se manejan bajo procedimientos internos teniendo en cuenta los siguiente items

1.1 Plan de Mantenimiento Preventivo

Incluye las actividades programadas semestral o anualmente para garantizar que los equipos tecnológicos operen en condiciones óptimas y comprende:

- Limpieza física y lógica.
- Revisión de parámetros técnicos.
- Actualización de firmware, parches y software.
- Verificación de rendimiento y estado de componentes.
- Pruebas de funcionamiento posterior a la intervención.

1.2 Plan de Mantenimiento Correctivo

Define el procedimiento para la atención de fallas inesperadas que afecten la disponibilidad de los servicios e incluye:

- Diagnóstico inmediato de la afectación.
- Priorización según criticidad del sistema.
- Intervención técnica para restablecer la operación.
- Registro de incidentes y causas raíz.
- Identificación de riesgos y acciones de ser necesarias.
- Acciones de mejora para prevenir recurrencias (cambios o reemplazo de partes afectadas).

1.3 Plan de Gestión de Activos Tecnológicos

Establece los lineamientos para identificar, registrar, clasificar y controlar los equipos sujetos a mantenimiento:

- Inventario actualizado de activos.
- Etiquetado y trazabilidad.
- Estado técnico de cada dispositivo.
- Relación con los servicios que soporta.
- Criterios para renovación o baja técnica.

1.4 Plan de Gestión de Riesgos Tecnológicos

Identifica posibles riesgos derivados de fallas, indisponibilidad o falta de mantenimiento, y define controles para mitigarlos:

- Evaluación de riesgos por tipo de activo.
- Definición de medidas preventivas.
- Análisis de impacto en la operación.
- Activación de planes alternos o contingencias.
- Registro y cierre de riesgos.

1.5 Plan de Mantenimiento de Infraestructura Crítica

Aplicado a los equipos del Centro de Datos y otros elementos de alta disponibilidad:

- UPS y sistemas de respaldo energético para el Centro de Datos.
- Aires acondicionados de precisión para el Centro de Datos.
- Gabinetes, bandejas y cableado estructurado.
- Equipos de seguridad perimetral y comunicaciones.

1.6 Plan de Ventanas de Mantenimiento

Define las franjas horarias y condiciones que permiten ejecutar mantenimientos sin afectar los servicios:

- Análisis de horas de baja demanda.
- Coordinación con líderes de procesos.
- Comunicación previa a los usuarios.
- Protocolos de cierre y reapertura de servicios.
- Verificación funcional posterior.

1.7 Plan de Evidencias y Documentación

Describe la forma en que deben registrarse y almacenarse las evidencias de mantenimiento en la herramienta de gestión de servicio:

- Evidencias técnicas o de software.
- Informes posteriores al mantenimiento.
- Archivo en el Sistema Integrado de Gestión.
- Trazabilidad para auditorías internas o externas.

1.8 Plan de Mejora Continua

Identifica oportunidades de optimización del proceso de mantenimiento:

- Evaluación anual de resultados.
- Identificación de fallas recurrentes.
- Actualización del cronograma según evolución tecnológica.
- Retroalimentación de proveedores y usuarios internos.
- Ajustes a procedimientos y tiempos de atención.

9 ACCIONES

Las acciones definidas en este pan incluyen los mantenimientos de la infraestructura física, las aplicaciones y las bases de datos, elementos técnicos y tecnológicos que soportan la operación diaria del Instituto:

1- Mantenimientos preventivos y correctivos de servidores, equipos de redes, comunicaciones, desarrollos, aplicaciones y bases de datos
2- Gestión e identificación de los activos de información donde se incluyen software, hardware e infraestructura crítica.
3- Gestión de riesgos tecnológicos que se documentan en la herramienta dispuesta por el Sistema Integrado de Gestión.
4- Definición de ventanas de mantenimiento donde se incluyen identificación de riesgos, retorno a la normalidad, partes interesadas, responsabilidades y tiempos estimados de acuerdo con las necesidades de la operación.
5- Documentación de las actividades y la mejora continua.

10 PLANES GENERALES DE COMPRAS QUE DESAGREGUEN LOS RECURSOS ASOCIADOS A TODAS LAS FUENTES DE FINANCIACIÓN

Teniendo en cuenta el PAA (Plan Anual de Adquisiciones), relacionado con los servicios de mantenimiento de la infraestructura técnica y tecnológica, presentamos la siguiente tabla con los valores y su fuente de inversión:

ELEMENTOS	FUENTE	VALOR	OBSERVACIONES
Equipos servidores	Inversión	$ 168.345.334	Contratistas
Equipos de Seguridad	Inversión	$ 1.999.688.274	Contrato de Servicios Tecnológicos Integrados
Equipos de Comunicaciones	Funcionamiento	$ 2.085.443.460	Contrato de Servicios Tecnológicos Integrados

ELEMENTOS	FUENTE	VALOR	OBSERVACIONES
Equipos de UPS yaires acondicionados del Centro de Datos	Inversión	$ 100.000.000	Contrato de Servicios Tecnológicos Integrados
Computadoresde Escritorio ComputadoresPortátiles	Inversión	$ 107.250.000	Contrato de Servicios Tecnológicos Integrados
Impresoras y Escáner	Inversión	--	En garantía
Bases de datos	Inversión	$ 222.744.600	Contratistas
Aplicaciones	Inversión	$ 452.436.400	Contratistas

11 INDICADORES

Id	Nombre	Proceso	Sentido	Tipo	Clasificación
443	Porcentaje de tickets atendidos con oportunidad, dentro los tiempos estipulados en la herramienta de gestión tecnológica	GESTIÓN DE LA INFRAESTRUCTURA Y SERVICIOS TECNOLÓGICOS	Hacia arriba	Eficiencia	Operativo
783	Asegurar la disponibilidad de los servicios tecnológicos, sistemas de información, bases de datos y telecomunicaciones para la normal operación del Invima.	GESTIÓN DE LA INFRAESTRUCTURA Y SERVICIOS TECNOLÓGICOS	Hacia arriba	Inversión	Operativo

Indicador 443 – Porcentaje de Tickets Atendidos con Oportunidad (Cumplimiento de SLA)

Definición: Porcentaje de tickets atendidos con oportunidad, dentro de los tiempos estipulados en la herramienta de gestión tecnológica, pactados hacia el Invima.

Fórmula: (Q Total de servicios en el mes / Q Servicios atendidos a tiempo)×100

Objetivo: Mayor o igual a **95%**

Objetivo ITIL / Necesidad: Este indicador evalúa el cumplimiento de los tiempos definidos en los **Acuerdos de Nivel de Servicio (SLA)**, un pilar esencial de la práctica de **Gestión de Niveles de Servicio** según ITIL. Su necesidad radica en asegurar que las solicitudes e incidentes se atiendan dentro de los plazos pactados, garantizando **previsibilidad, eficiencia operativa y atención priorizada**. Monitorear este indicador permite medir la capacidad real del soporte para responder oportunamente y mantener la confianza institucional en la gestión tecnológica.

Indicador 783 – Disponibilidad de los Servicios Tecnológicos

Definición: Asegurar la disponibilidad de los servicios tecnológicos, sistemas de información, bases de datos y telecomunicaciones para la normal operación del Invima.

Fórmula: (Tiempo de actividad / Tiempo total)×100

Objetivo: Mayor o igual a **95%**

Objetivo ITIL / Necesidad: Este indicador refleja la capacidad de la infraestructura tecnológica para **mantener los servicios operando sin interrupciones**, un principio fundamental en ITIL dentro de la práctica de **Gestión de Disponibilidad**. Su necesidad radica en garantizar la **continuidad del servicio**, minimizar impactos operativos y asegurar que los usuarios puedan ejecutar sus actividades sin fallos que afecten la misión institucional. Una alta disponibilidad es esencial para sostener la eficiencia, la confiabilidad y el valor del servicio tecnológico.

12 CRONOGRAMA

Ver archivo adjunto **PLAN DE MANTENIMIENTO DE SERVICIOS TECNOLÓGICOS 2026**

13 MAPAS DE RIESGOS

Se presenta el detalle de los riesgos identificados y documentados en nuestro sistema integrado de gestión, relacionados con los planes de mantenimiento:

Riesgo Identificado: 1267

Nombre del Riesgo: Posibilidad de afectación de la operación de la entidad, por la indisponibilidad del activo de información, debido a las fallas de software y hardware del centro de datos;

Descripción: Imposibilidad de acceso a la información por parte de la entidad cuando se presente una falla en la infraestructura y herramientas tecnológicas del centro de datos (hardware y software)

Alcance: Todo el Instituto

Procesos: GESTIÓN DE LA INFRAESTRUCTURA Y SERVICIOS TECNOLÓGICOS

Causas:

1. Difusión de software dañino (Malware, virus, ransomware) (origen: Interno, factor: Estructura)
2. Incumplimientos en los objetivos contratados o en los acuerdos de niveles de servicios (origen: Interno, factor: Estructura)
3. No renovación de contratos oportunamente (origen: Interno, factor: Estructura)
4. Fallas en los equipos tecnológicos y/o eléctricos (fallas eléctricas, inundaciones, etc.) (origen: Interno, factor: Estructura)
5. Afectación de los sistemas o la infraestructura como consecuencia de una actualización (origen: Interno, factor: Recursos)
6. Falta de mantenimiento de los equipos tecnológicos y eléctricos en el centro de datos (origen: Interno, factor: Recursos)
7. Incumplimientos en los objetivos contratados o en los acuerdos de niveles de servicios (origen: Externo, factor: Legal / Reglamentario)
8. Ataque a las vulnerabilidades de los sistemas informáticos de la Entidad que pueden afectar la operación del servicio (origen: Externo, factor: Tecnológico)
9. Corte de suministro de energía del proveedor (origen: Externo, factor: Tecnológico)

Efectos:

- Perdida de información
- Demoras en los procesos y/o operación
- Incremento de costos
- Atención parcial o nula al ciudadano
- Pérdida de imagen Institucional
- Insatisfacción de los usuarios internos del Invima
- Daños irreversibles en equipos tecnológicos y herramientas tecnológicas
- Disminución o pérdida de productividad

Control 1 - Realizar la gestión de PQRDs para TICS

El funcionario delegado por la Oficina de Tecnologías de la Información, cada vez que se asigne una PQRDS relacionada con el riesgo, verifica la información solicitada y da respuesta al peticionario en los términos legales vigentes, lo cual se puede evidenciar en el aplicativo de correspondencia de la entidad, de acuerdo a lo establecido en el procedimiento para la gestión de peticiones, quejas, reclamos, denuncias y sugerencias.

En caso de encontrar observaciones o desviaciones en el desarrollo del control, se informa al líder de proceso para la investigación y el tratamiento pertinente dentro de los tiempos de ley establecidos.

Control 2 - Gestionar los hallazgos identificados en auditorías internas y externas

El funcionario delegado por la Oficina de Tecnologías de Información, una vez sea identificado un hallazgo relacionado con el riesgo, verifica la información para llevar a cabo las actividades de mejoramiento continuo, en los instrumentos del sistema de gestión integrado de acuerdo a lo establecido en el procedimiento de Acciones de mejora.

En caso de encontrar observaciones o desviaciones en el desarrollo del control, se informa al líder de proceso y se comunica a las partes interesadas que participan de las actividades para dar el tratamiento correspondiente, de acuerdo con el resultado del análisis de causas.

Control 3 - Monitorear la disponibilidad de los equipos tecnológicos, infraestructura y servidores de misión crítica del centro de datos.

El funcionario designado por el Grupo de Soporte Tecnológico monitorea continuamente la disponibilidad y el estado operativo de los equipos tecnológicos, infraestructura y servidores de misión crítica del centro de datos, mediante herramientas automatizadas que generan reportes diarios de eventos y alertas. Las acciones están documentada en el procedimiento **Administración del Centro de Datos**, y se evidencia con los reportes diarios de disponibilidad y alertas técnicas.

Este control sirve para garantizar la continuidad operativa y la disponibilidad de los servicios tecnológicos críticos del Invima, lo cual es fundamental tanto para la gestión institucional como para la prevención de riesgos de corrupción y fallas operativas.

Las causas asociadas a este control son:

- Fallas en los equipos tecnológicos y/o eléctricos (fallas eléctricas, inundaciones, etc.)

- Afectación de los sistemas o la infraestructura como consecuencia de una actualización
- Ataque a las vulnerabilidades de los sistemas informáticos de la Entidad que pueden afectar la operación del servicio
- Corte de suministro de energía del proveedor

Control 4 - Realizar mantenimiento a la infraestructura de los servidores

El funcionario delegado por el Grupo de Infraestructura Tecnológica coordina y supervisa la ejecución de mantenimientos preventivos y correctivos a la infraestructura de servidores de misión crítica, con el fin de garantizar su estabilidad, disponibilidad y cumplimiento de los niveles de servicio establecidos. Estas actividades son realizadas por proveedores especializados contratados por la Entidad, quienes ejecutan actualizaciones, validaciones técnicas y entregan reportes periódicos de las intervenciones realizadas. El control está documentado en el procedimiento **Administración del Centro de Datos**, y se evidencia mediante los informes técnicos de mantenimiento, registros de intervención y reportes de validación entregados por los contratistas.

Este control permite asegurar la continuidad operativa de los servicios institucionales y mitigar riesgos asociados a fallas técnicas o indisponibilidad de la infraestructura.

Las causas asociadas a este control son:

- Incumplimientos en los objetivos contratados o en los acuerdos de niveles de servicios
- No renovación de contratos oportunamente
- Falta de mantenimiento de los equipos tecnologicos y electricos en el centro de datos
- Incumplimientos en los objetivos contratados o en los acuerdos de niveles de servicios

Control 5 - Activar el mantenimiento preventivo de UPS y componentes eléctricos

El funcionario asignado del Grupo de Soporte Tecnológico es responsable de coordinar y supervisar el mantenimiento preventivo de las UPS y demás componentes eléctricos del Centro de Datos. Estas actividades se realizan al menos una vez al año, o según lo establecido en los servicios contratados y las garantías del proveedor. El proveedor debe entregar un informe técnico de cada mantenimiento a los administradores del Centro de Datos, en cumplimiento del contrato vigente y conforme al procedimiento de administración del centro de Datos.

Este control busca garantizar la continuidad operativa y mitigar riesgos asociados a fallas eléctricas.

Las causas asociadas a este control son:

- Incumplimientos en los objetivos contratados o en los acuerdos de niveles de servicios
- No renovación de contratos oportunamente
- Fallas en los equipos tecnológicos y/o eléctricos (fallas eléctricas, inundaciones, etc.)
- Falta de mantenimiento de los equipos tecnológicos y eléctricos en el centro de datos
- Incumplimientos en los objetivos contratados o en los acuerdos de niveles de servicios
- Corte de suministro de energía del proveedor

Control 6 - Monitorear y mantener herramientas para control ataques informáticos

El funcionario delegado por el Grupo de Soporte Tecnológico realiza el monitoreo diario y la gestión técnica de las herramientas de protección contra software malicioso, con el fin de detectar, prevenir y mitigar ataques informáticos que puedan comprometer la seguridad de los sistemas institucionales. Este control incluye la supervisión del funcionamiento del antivirus corporativo y otras soluciones de seguridad, así como la revisión de logs, reportes de eventos y tickets generados en la herramienta de gestión de mesa de servicios. La actividad está documentada en el procedimiento **Administración del Centro de Datos**, y se evidencia mediante los registros de monitoreo, reportes de eventos y trazabilidad de acciones correctivas. Este control permite proteger la infraestructura tecnológica del Invima frente a amenazas digitales y garantizar la integridad de la información institucional.

Las causas asociadas a este control son:

- Difusión de software dañino (Malware, virus, ransomware)
- Fallas en los equipos tecnológicos y/o eléctricos (fallas eléctricas, inundaciones, etc.)
- Afectación de los sistemas o la infraestructura como consecuencia de una actualización
- Ataque a las vulnerabilidades de los sistemas informáticos de la Entidad que pueden afectar la operación del servicio

Riesgo Identificado: 1269

Nombre del Riesgo; Posibilidad de afectación en la operación de la entidad por entrega inoportuna de los desarrollos nuevos y/o ajustes de los sistemas de información debido al alto volumen de solicitudes y falta de personal para su atención.

Descripción; Entrega inoportuna de los ajustes o desarrollos nuevos en los aplicativos de la entidad

Alcance; Todo el Instituto

Procesos; GESTIÓN INFORMATICA Y DE LA INFORMACIÓN

Causas

1 Requerimientos adicionales al proyecto que afectan el desarrollo (origen: Interno, factor: Recursos)
2 Otras prioridades que surgen de decisiones gerenciales, etc (origen: Interno, factor: Recursos)
3 Falta de personal para la atención y solución de requerimientos (origen: Interno, factor: Recursos)
4 Ataques cibernéticos que afecten las infraesturura Tecnologica (origen: Interno, factor: Recursos)
5 Por cambios en la normatividad que implican modificaciones en los aplicativos (origen: Externo, factor: Político)
6 Incumplimiento de las obligaciones contractuales por parte de los contratistas o proveedores (origen: Externo, factor: Legal / Reglamentario)

Efectos

- Sanciones en contra de Invima
- Insatisfacción de los funcionarios y usuarios
- Demoras en los trámites del Invima
- Detrimento de la Imagen institucional por las quejas y/o reclamos de los usuarios externos
- Retrasos en el cumplimiento de los entregables en la operación misional

Control 1 - Realizar la gestión de PQRDs para TICS

El funcionario delegado por la Oficina de Tecnologías de la Información, cada vez que se asigne una PQRDS relacionada con el riesgo, verifica la información solicitada y da respuesta al peticionario en los términos legales vigentes, lo cual se puede evidenciar en el aplicativo de correspondencia de la entidad, de acuerdo a lo establecido en el procedimiento para la gestión de peticiones, quejas, reclamos, denuncias y sugerencias.

En caso de encontrar observaciones o desviaciones en el desarrollo del control, se informa al líder de proceso para la investigación y el tratamiento pertinente dentro de los tiempos de ley establecidos.

Causa asociada:

- Incumplimiento de las obligaciones contractuales por parte de los contratistas o proveedores

Control 2 - Gestionar los hallazgos identificados en auditorías internas y externas

El funcionario delegado por la Oficina de Tecnologías de Información, una vez sea identificado un hallazgo relacionado con el riesgo, verifica la información para llevar a cabo las actividades de mejoramiento continuo, en los instrumentos del sistema de gestión integrado de acuerdo a lo establecido en el procedimiento de Acciones de mejora.

En caso de encontrar observaciones o desviaciones en el desarrollo del control, se informa al líder de proceso y se comunica a las partes interesadas que participan de las actividades para dar el tratamiento correspondiente, de acuerdo con el resultado del análisis de causas.

Las causas asociadas a este control son:

- Requerimientos adicionales al proyecto que afectan el desarrollo
- Por cambios en la normatividad que implican modificaciones en los aplicativos

Control 3 - Aprobar solicitudes de cambios o requerimientos tecnológicos

El Director o Jefe de Oficina solicitante, el Jefe de la Oficina Asesora de Planeación, el Jefe de la Oficina Asesora Jurídica y el Jefe de la Oficina de Tecnologías de la Información aprueban toda solicitud de cambio o requerimiento tecnológico, según procedimiento TIC-GIN-PR001, respaldado mediante el formato correspondiente con las firmas de aprobación. El control se activa cada vez que se presenta una solicitud, garantizando la trazabilidad, validación técnica, jurídica y estratégica de los cambios propuestos.

Las causas asociadas a este control son:

- Requerimientos adicionales al proyecto que afectan el desarrollo
- Otras prioridades que surgen de decisiones gerenciales, etc
- Falta de personal para la atención y solución de requerimientos
- Por cambios en la normatividad que implican modificaciones en los aplicativos

Control 4 - Responder viabilidad de implementación de requerimientos tecnológicos

El funcionario designado de la Oficina de Tecnologías de la Información (OTI) analiza la viabilidad de cada solicitud relacionada con cambios o implementaciones tecnológicas que puedan impactar la operación del centro de datos. Esta evaluación se realiza conforme al procedimiento y se aplica cada vez que se recibe una solicitud. Como evidencia del control, se genera una comunicación formal al solicitante con el resultado del análisis, y se registra la gestión en la plataforma Aranda.

Este control permite anticipar riesgos técnicos, asegurar la continuidad operativa y garantizar decisiones informadas sobre la infraestructura tecnológica.

Las causas asociadas a este control son:

- Requerimientos adicionales al proyecto que afectan el desarrollo
- Otras prioridades que surgen de decisiones gerenciales, etc
- Falta de personal para la atención y solución de requerimientos
- Por cambios en la normatividad que implican modificaciones en los aplicativos

- Ataques cibernéticos que afecten la infraestructura Tecnológica
- Incumplimiento de las obligaciones contractuales por parte de los contratistas o proveedores

Control 5 - Supervisar la ejecución del contrato

El funcionario designado de la Oficina de Tecnologías de la Información (OTI) designa un supervisor responsable del seguimiento y control de la ejecución del contrato, conforme a lo establecido en el procedimiento.

Esta actividad se realiza cada vez que se suscribe un contrato que lo requiera, y queda debidamente documentada. El control permite verificar el cumplimiento de las obligaciones contractuales, garantizar la calidad del servicio o bien contratado y asegurar la trazabilidad de la gestión contractual.

Las causas asociadas a este control son:

- Otras prioridades que surgen de decisiones gerenciales, etc
- Por cambios en la normatividad que implican modificaciones en los aplicativos
- Incumplimiento de las obligaciones contractuales por parte de los contratistas o proveedores