enterritorio
Empresa Nacional Promotora del Desarrollo Territorial S.A.

Al contestar por favor cite estos datos:
Radicado No.: 202518010004293

Pública ☐ **Pública Reservada** ☐ **Pública Clasificada** ☐

MEMORANDO

Bogotá D.C, 30-09-2025 08:55:31

PARA: ARMANDO VIVAS SALAMANCA
Gerente tecnologías de la Información

DE: ORLANDO CORREA NÚÑEZ
Asesor de Control Interno

ASUNTO: Notificación informe definitivo de la auditoría gestión de Tecnologías de información

Cordial saludo Ingeniero Armando

En cumplimiento del plan anual de auditoría 2025 y del procedimiento P-AU-01, la Asesoría de Control Interno socializa el resultado definitivo de la auditoría realizada al proceso Gestión de Tecnologías de información. Es de anotar que no se recibió retroalimentación al informe preliminar notificado con radicado N. 202518010004203 del 23/09/2025.
Anexo a este memorando, se envía: El formato F-AU-28 Evaluación equipo auditor, con el fin de ser diligenciado en particular, por quienes acompañaron el proceso de la auditoría.

De igual manera, a partir de la fecha de la presente comunicación, el grupo de Gestión de TI y áreas que corresponda, disponen de 10 días hábiles, para formular el plan de mejoramiento junto con el respectivo análisis de causas, esto es hasta el 14 de octubre 2025

Cordialmente,

Firmado Digitalmente por
ORLANDO CORREA NUÑEZ
Fecha: 30-09-2025 08:55:33
AM

ORLANDO CORREA NUÑEZ
ASESOR DE CONTROL INTERNO

Proyectó: CELENY GONZALEZ PARRA - CONTRATISTA - ASESORIA DE CONTROL INTERNO
Elaboró: CELENY GONZALEZ PARRA - CONTRATISTA - ASESORIA DE CONTROL INTERNO
Adjuntos: F-AU-29_V01 Formato Informe Definitivo.pdf(30)

enterritorio Empresa Nacional Promotora del Desarrollo Territorial S.A.	**INFORME DEFINITIVO-TRABAJOS DE ASEGURAMIENTO**	CÓDIGO:	**F-AU-29**
		VERSIÓN:	**01**
		VIGENCIA:	**2025-06-12**
	AUDITORÍA INTERNA	CLASIFICACIÓN	**IP**

FECHA:	**29/09/2025**
PROCESO/ UNIDAD AUDITADA:	Gestión de Tecnologías de la Información
RESPONSABLE DIRECTIVO:	Armando Vivas Salamanca Gerente Tecnologías de la Información
EQUIPO AUDITOR:	Celeny González Parra

OBJETIVO:

Evaluar y hacer seguimiento a la adecuada gestión de riesgos y aplicación de las actividades y controles claves asociados al PROCESO de Gestión de las Tecnologías de la Información, a través de los procedimientos internos establecidos, y normatividad aplicable

ALCANCE:

Periodo entre julio 2024 a julio 2025

FORTALEZAS

1. Uso de la herramienta de gestión Aranda para el registro de los requerimientos de los usuarios y/o cambios /mantenimientos a los componentes tecnológicos
2. Comité semanal de cambios del equipo de tecnologías de la información y el operador Tecnológico, para el seguimiento de los cambios de la plataforma tecnológica
3. Acompañamiento técnico por parte de Gestión de tecnologías de la Información en la etapa de planeación para contratos de mantenimiento o actualización de software

OPORTUNIDADES DE MEJORA

1. Se observó falta de estandarización en la identificación, contenido y estructura de los soportes documentales de las fases de desarrollo de software en relación con la guía vigente.
2. Para el análisis de los cambios realizados a los componentes tecnológicos se observó el uso del formato control de cambios el cual no está formalizado en el sistema de gestión, tampoco se menciona en el procedimiento de cambios.
3. Se observaron diferencias en las actividades descritas en el procedimiento de control de cambios frente a las actividades ejecutadas y recolección de soportes o evidencias

4. Los casos particulares o excepciones frente a la aplicación de los procedimientos o actividades, no se encuentran documentados o descritos en estos.
5. En los informes de gestión mensuales presentados por el operador tecnológico, solicitar la estandarización en la presentación de los resultados de los monitoreos y precisar las gestiones realizadas.
6. Se evidenció que no se lleva registro de ingreso a los diferentes racks de comunicaciones de los pisos, solo se aplica para el ingreso al centro de cómputo del piso 28
7. Frente a las necesidades de software o componentes tecnológicos solicitados a las áreas para cada vigencia, no se observó retroalimentación o respuesta emitida por Gestión de tecnologías de la información, frente a estos requerimientos, a su vez, es importante definir y documentar las variables analizadas para priorizar el presupuesto de cada vigencia.

OBSERVACIONES IDENTIFICADAS

CONDICIÓN:	Observación 1. Deficiencias en el diseño de controles Se evidenciaron deficiencias en la definición y diseño de los siguientes controles: 1.CTROPETI-27: el objetivo del control no está relacionado con la descripción del control, toda vez que el control refiere a determinar " *si el aplicativo será adquirido o desarrollado internamente.* " y el objetivo del control refiere al correcto funcionamiento de los nuevos aplicativos. No establece la instancia o rol de aprobación para cualquiera de las dos opciones: desarrollarlo internamente o adquirirlo. 2.CTROPETI-36: La descripción del control no incluye una acción orientada en revisar, validar, cotejar, comparar, aprobar, entre otras, y la periodicidad de seguimiento/aprobación semanal del comité de cambios. A su vez, la segunda parte del control CTROPETI-36 , que indica **"**Adicionalmente, se cuenta con una metodología para el mantenimiento de aplicativos que se encuentran en producción", puede ser unificado con el CTROPETI-3 "Mantenimiento de aplicaciones" y/o con el control CTROPETI-12 "Metodología estándar para el desarrollo y/o mantenimiento de aplicativos". 3.CTROPETI-12: La descripción del control *indica "evaluar las necesidades por parte del líder de desarrollo y dar iniciar la solución en caso de ser viable"* , no contiene lo referido en el nombre "Metodología estándar para el desarrollo y/o mantenimiento de aplicativos". 4.CTROPETI-23: En el atributo "documentación" de la matriz SIAR, registra "sin documentar", sin embargo, en el M-RI-06 MANUAL DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN v.6 , numeral 9.1 Perímetro de seguridad física, define la política. En la descripción del control indica "En algunos centros de cableado (...) " lo cual resulta ambiguo para la aplicación y verificación de cumplimiento del control.

	5.CTROPETI-40: En la definición del control, no se hace referencia a las herramientas automáticas implementadas para realizar el monitoreo a la plataforma tecnológica y el uso permanente de estas. En la Matriz SIAR en los atributos: RELACIÓN DE DOCUMENTACIÓN: solo se relaciona el procedimiento P-RI-20 Creación y administración de roles y privilegios de los usuarios de los servicios tecnológicos, sin embargo, también aplicaría el procedimiento de cambios, y el "ANEXO TÉCNICO No. 2 – SERVICIOS DE SEGURIDAD TECNOLÓGICA" del operador tecnológico EVIDENCIA: está catalogado como material, sin embargo, se trata de un registro sustancial (logs y alertas) ; a su vez en los soportes, complementar con los informes del operador tecnológico donde se presentan los análisis de los eventos detectados por periodo. RELACIÓN DE SOPORTES: solo incluye Caso radicado en Aranda, sin embargo, un soporte relevante es el informe mensual del operador tecnológico donde se presentan los análisis de los eventos detectados por periodo. 6. CRLAF63: la descripción no tiene las características de un control, toda vez que “realizar un informe " es una actividad. Un control debe contener una acción orientada en revisar, validar, cotejar, comparar, aprobar, entre otras
CRITERIO:	G-RI-04 GUÍA METODOLÓGICA DE GESTIÓN DE RIESGOS Numeral 4.6.1.2 MEDICIÓN DE LA EFICIENCIA INDIVIDUAL DEL CONTROL SIAR
CAUSA PROBABLE:	Para la actualización de los controles en su diseño y atributos, no se tienen en cuenta integralmente los procedimientos o guías del proceso, y las características propias de un control
RIESGO	ROPERI-13 Debilidades en el monitoreo de los riesgos de la Sociedad
CONSECUENCIA:	Limitación para monitorear de manera efectiva la aplicación de los controles
RECOMENDACIÓN(ES):	Revisar y ajustar la definición de los controles y sus objetivos, de tal forma que cumplan con las características de un control, esto implica considerar la claridad del propósito del control (verificar, validar, cotejar, conciliar, etc.), a su vez ajustar los atributos del diseño según corresponda, en concordancia con los procedimientos vigentes y soportes de ejecución de las actividades.
NIVEL CRITICIDAD	Moderado

CONDICIÓN:

Observación 02. Deficiencias en la trazabilidad y registro del ciclo de desarrollo de software

Producto de la revisión de los documentos soporte para cada fase de desarrollo para los 5 casos revisados:

Caso N.	Descripción	área usuaria
18286	aplicativo de liquidaciones	Gestión poscontractual
19995	Aerocivil	Subgerencia de Desarrollo de Proyectos
20606	Registro de encuesta para contratistas	Transversal
20629	Tablero de control Gestiones pendientes por Grupos de Trabajo LIRA	Servicios Administrativos Transversal
20694	Operaciones Inusuales	SARLAFT

Fuente: Elaboración ACI

Se identificaron las siguientes situaciones:

a. DEBILIDADES EN FASE DE ANÁLISIS Y LEVANTAMIENTO DE INFORMACIÓN
Para ningún caso se evidenció el "Equipo que trabajará en el proyecto" con la definición de los roles, las responsabilidades y el tiempo de disponibilidad de cada una de las personas del equipo.
El formato F-T11 definición de requerimiento de software, para los casos 19995 y 20606 no se encuentran firmado por el usuario líder y para el caso 20629 no evidenció la suscripción.
Para el caso 18286 no se observó la definición de aspectos no funcionales
Todos los casos están registrados en la herramienta Aranda y fueron aportados los cronogramas o plan de trabajo, excepto para el caso 20629-Tablero control Lira. Sin embargo, el cronograma presentado no está definido para cada una de las fases del desarrollo.
b. FASE DE DISEÑO
Para el caso 20629 no se evidenció el documento con el diseño lógico del desarrollo
c. DEBILIDADES EN LA FASE DESARROLLO

	En el repositorio documental para esta fase, se aportaron soportes de provisionamiento o creación de recursos para ambiente de desarrollo para los casos:20694, 19995 y 20606. Sin embargo, estos corresponden a correos de solicitud enviados, sin disponer de los soportes que den cuenta de la creación de estos ambientes. d. DEBILIDADES EN LA FASE IMPLEMENTACION En el repositorio documental para esta fase se aportaron 19995, 20606, 20694 de provisionamiento o creación de ambientes de pruebas, Sin embargo, estos corresponden a correos de solicitud enviados, sin disponer de los soportes que den cuenta de la creación de estos ambientes. F-TI-22 Pruebas de calidad de software, debidamente diligenciado: Para el caso 18286 el documento aportado no se encuentra integralmente diligenciado, y registra resultado del caso" no aprobado", y para el caso 20629 no se evidenció su elaboración. No contar con la documentación de las pruebas ejecutadas exitosamente, puede conllevar a errores funcionales o de rendimiento en la etapa de producción. Caso en la herramienta de Gestión documentado de las evidencias de las pruebas de usuario: no aportado para el caso 18286, y para el caso 20694 a la fecha de verificación 11/09/2025 se encuentran en ejecución las pruebas por parte del usuario. e. DEBILIDADES FASE DE PASO A PRODUCCIÓN Documentación de instalación de ambiente de producción: Para el caso 20629 no se evidenció este soporte. Registro en la herramienta de Gestión conforme al procedimiento P-TI-06: para los casos 18286 y 19995 se observó el acta de comité de cambios donde se socializó el paso a producción. Para el caso 20606 y 20629 no se observaron estos soportes. Guía Técnica y de usuario, y el correo electrónico que permita evidenciar comunicación entre el Ingeniero de Desarrollo y el Usuario: ´no se evidenciaron estos documentos para el caso 20629. f. DEBILIDAD EN LA DOCUMENTACIÓN DEL CICLO DE DESARROLLO En el repositorio documental para cada fase del ciclo de desarrollo de software , se observó falta de estandarización e identificación del soporte definitivo para cada producto o entregable definido en la guía G-TI-02_V05 Desarrollo, ajuste y estandarización de software v.5, debido a que se aportaron múltiples documentos como correos, citaciones a reuniones, varias versiones del mismo documento (ej. F-TI-11) u otros, que dificultan la identificación del soporte que da cuenta de la ejecución de cada actividad.
CRITERIO:	G-TI-02 DESARROLLO, AJUSTE Y ESTANDARIZACIÓN DE SOFTWARE Alcance: La metodología abarca actividades que deben ejecutarse sistemáticamente, documentando lo realizado por parte de los integrantes del proyecto y los resultados tangibles en forma de programas y de los documentos que deben originarse. Este documento se ha dividido en fases, las cuales presentan conceptos generales de sistemas de información y la metodología como tal, donde se describen las fases del ciclo de vida de los proyectos de sistemas de información así: análisis y levantamiento de información, diseño, desarrollo, implementación y paso a producción. CTROPETI-12 Metodología estándar para el desarrollo y/o mantenimiento de aplicativos
CAUSA PROBABLE:	Falta de estandarización en los soportes y seguimiento a las etapas del ciclo de desarrollo de software

	Vacíos en los procedimientos documentados, al no incluir condiciones particulares o posibles excepciones que pueden aplicar
RIESGOS	ROPETI-4: Inoportunidad en la atención de requerimientos de actualización, desarrollo, mejora a los sistemas de información o soporte tecnológico ROPETI-9 Daño o malfuncionamiento del hardware o software
CONSECUENCIA:	Afecta el seguimiento y monitoreo de las fases de desarrollo y puesta en producción de software, debido a que no se identifica específicamente el soporte final o definitivo de cada actividad, o en su defecto en algunos casos no se cuenta con soporte que evidencie la ejecución, soportes vitales para la etapa de mantenimiento. A su vez genera reprocesos al interior del grupo de trabajo para atender requerimientos de entes de control interno y/o externos
RECOMENDACIÓN(ES):	Documentar los casos de desarrollo de acuerdo con la guía G-TI-02 DESARROLLO, AJUSTE Y ESTANDARIZACIÓN DE SOFTWARE para cada fase tomando en consideración los numerales "*Tareas a realizar"* y *"productos a obtener"* , estandarizando su identificación y soportes definitivos validados en su integridad y completitud, que den cuenta del cumplimiento de cada ítem. Verificar las condiciones generales de la guía G-TI-02 DESARROLLO, AJUSTE Y ESTANDARIZACIÓN DE SOFTWARE y del procedimiento P-TI-04_V05 Desarrollo, mantenimiento y puesta en producción de software, a fin de establecer los lineamientos para aquellos casos que no le apliquen las reglas generales.
NIVEL CRITICIDAD	MODERADO

CONDICIÓN:	Observación 3. Deficiencias en el registro y seguimiento al control de cambios de los componentes tecnológicos De acuerdo con el procedimiento P.TI-06 CONTROL DE CAMBIOS A LA INFRAESTRUCTURA TECNOLÓGICA V.5, se validaron las siguientes actividades frente a "REGISTROS/ EVIDENCIAS" 1.Clasificación del cambio y la solución técnica, considerando los factores costo/beneficio, viabilidad y riesgo para el negocio (actividad 1- acta de reunión) De los 15 casos revisados, dos no les aplicó este ítem, y para los 13 (87%) restantes no se observó el acta de reunión, así:

Número del caso	**Categoría**	Verificación
1675	Red Cableada	N.A, no es un cambio es una actividad
1760	Red Cableada	No existe evidencia de la ejecución de la actividad 1 "Identificación de la necesidad de realizar un cambio, Se analiza la clasificación del cambio y la solución técnica, considerando los factores costo/beneficio, viabilidad y riesgo para el negocio.", del procedimiento P-TI.06 CONTROL DE CAMBIOS A LA INFRAESTRUCTURA TECNOLÓGICA, cuya evidencia o soporte es "ACTA REUNION"
17941	TIQUETES Mantenimiento aplicación	De acuerdo con la descripción del control 36, "según la naturaleza del cambio presentado o por evento, se analiza el impacto y su afectación en estructuras de bases de datos o código, y se determina su viabilidad. (Adquisición, desarrollo y puesta en producción de software)", para este caso no se evidenció este análisis, tampoco se observó el F-TI-11 requerimiento de Software. No existe evidencia de la ejecución de la actividad 1 "Identificación de la necesidad de realizar un cambio, Se analiza la clasificación del cambio y la solución técnica, considerando los factores costo/beneficio, viabilidad y riesgo para el negocio.", del procedimiento P-TI.06 CONTROL DE CAMBIOS A LA INFRAESTRUCTURA TECNOLÓGICA, cuya evidencia o soporte es "ACTA REUNION"
17981	GEOTEC – FONVIVIENDA Mantenimiento aplicación	De acuerdo con la descripción del control 36, *"según la naturaleza del cambio presentado o por evento, se analiza el impacto y su afectación en estructuras de bases de datos o código, y se determina su viabilidad. (Adquisición, desarrollo y puesta en producción de software)"* Se observó el F-TI-11 requerimiento de Software firmado por el usuario líder. Aunque se observó la confirmación de ejecución correcta del script en la base de datos SIIF producción, no se aportó el análisis previo de impactos en la base de datos del cambio a realizar, como tampoco el acta de reunión en cumplimiento de la actividad 1 del procedimiento control de cambios.
1993	Firewalls	Aunque se aportó el FORMATO CONTROL DE CAMBIOS, este soporte no corresponde al definido en la actividad 1 "Identificación de la necesidad de realizar un cambio", del procedimiento P-TI.06 CONTROL DE CAMBIOS A LA INFRAESTRUCTURA TECNOLÓGICA, cuya evidencia o soporte es "ACTA REUNION"
2005	Unidades de Almacenamiento	No existe evidencia de la ejecución de la actividad 1 "Identificación de la necesidad de realizar un cambio, Se analiza la clasificación del cambio y la solución técnica, considerando los factores costo/beneficio, viabilidad y riesgo para el negocio.", del procedimiento P-TI.06 CONTROL DE CAMBIOS A LA INFRAESTRUCTURA TECNOLÓGICA, cuya evidencia o soporte es "ACTA REUNION"

2012	Servidores Virtuales	No existe evidencia de la ejecución de la actividad 1 "Identificación de la necesidad de realizar un cambio, Se analiza la clasificación del cambio y la solución técnica, considerando los factores costo/beneficio, viabilidad y riesgo para el negocio.", del procedimiento P-TI.06 CONTROL DE CAMBIOS A LA INFRAESTRUCTURA TECNOLÓGICA, cuya evidencia o soporte es "ACTA REUNION"
2019	Servidores Virtuales	Se observó el acta 18 del 22-05-2025, que en la Sección COMPROMISOS ACTA 17 (2025/05/15) indica "*A17: Cambio versión emails_out 5.2 a 5.3: Actualización de versión del servicio en nodo de componentes, no tiene afectación (Carolina Ardila). Pruebas por parte del ingeniero Wilson Cobos. A18: Se ejecuto de manera satisfactoria cambio 2019"*. También se observó el Formato de control de cambios, como soporte del análisis del caso, sin embargo, no corresponde al soporte definido en la actividad 1 del procedimiento P-TI.06 CONTROL DE CAMBIOS A LA INFRAESTRUCTURA TECNOLÓGICA
2055	Servidores Virtuales	Si bien se aportó el formato de control de cambios, no existe evidencia de la ejecución de la actividad 1 "Identificación de la necesidad de realizar un cambio, Se analiza la clasificación del cambio y la solución técnica, considerando los factores costo/beneficio, viabilidad y riesgo para el negocio.", del procedimiento P-TI.06 CONTROL DE CAMBIOS A LA INFRAESTRUCTURA TECNOLÓGICA, cuya evidencia o soporte es "ACTA REUNION"
2068	Unidades de Almacenamiento	No existe evidencia de la ejecución de la actividad 1 "Identificación de la necesidad de realizar un cambio, Se analiza la clasificación del cambio y la solución técnica, considerando los factores costo/beneficio, viabilidad y riesgo para el negocio.", del procedimiento P-TI.06 CONTROL DE CAMBIOS A LA INFRAESTRUCTURA TECNOLÓGICA, cuya evidencia o soporte es "ACTA REUNION"
2097	Firewalls	En mesa de trabajo del 16/09/2025, se presentó y se aportó el formato "RFC Cambio - Update FW CCB versión 7-4-8", el cual contiene la descripción general y específica, riesgos de ejecución del cambio, entre otros, En el acta 27 del 2025-07-24, registra "A24: Update Firewall CCB. Actualización de Firmware del firewall sede CCB de la versión 7.4.6 a la versión 7.4.8. Cambio 2097 autorizado para el 8 de julio de 2025 a las 22:00." Y también registra "A27: Se da cierre al cambio debido a que fue fallido. Es necesario realizar un rollback a la versión 7.4.6" Sin embargo, el soporte la primera actividad del procedimiento P-TI-06 "Se analiza la clasificación del cambio y la solución técnica, considerando los factores costo/beneficio, viabilidad y riesgo para el negocio" es Acta de reunión y no el formato RFC
2101	Seguridad Perimetral	Si bien se aportó el formato de control de cambios, no existe evidencia de la ejecución de la actividad 1 "Identificación de la necesidad de realizar un cambio, Se analiza la clasificación del cambio y la solución técnica, considerando los factores costo/beneficio, viabilidad y riesgo para el negocio.", del procedimiento P-TI.06 CONTROL DE CAMBIOS A LA INFRAESTRUCTURA TECNOLÓGICA, cuya evidencia o soporte es "ACTA REUNION"

2123	Firewalls	No existe evidencia de la ejecución de la actividad 1 "Identificación de la necesidad de realizar un cambio, Se analiza la clasificación del cambio y la solución técnica, considerando los factores costo/beneficio, viabilidad y riesgo para el negocio.", del procedimiento P-TI.06 CONTROL DE CAMBIOS A LA INFRAESTRUCTURA TECNOLÓGICA, cuya evidencia o soporte es "ACTA REUNION"
2132	Servidores Virtuales	N.A, no es un cambio es una actividad
19905	Sistema Control de asistencia Mantenimiento aplicación	De acuerdo con la descripción del control 36, *"según la naturaleza del cambio presentado o por evento, se analiza el impacto y su afectación en estructuras de bases de datos o código, y se determina su viabilidad. (Adquisición, desarrollo y puesta en producción de software)"* Se observaron : *F-TI-11 requerimiento de Software firmado por el usuario líder * FORMATO RFC UT - ENTERRITORIO_v0 - control de cambios *Evidencias despliegue ControlAsistencia-wsENT_07062025: cambios técnicos realizados Sin embargo, no existe evidencia de la ejecución de la actividad 1 "Identificación de la necesidad de realizar un cambio, Se analiza la clasificación del cambio y la solución técnica, considerando los factores costo/beneficio, viabilidad y riesgo para el negocio.", del procedimiento P-TI.06 CONTROL DE CAMBIOS A LA INFRAESTRUCTURA TECNOLÓGICA, cuya evidencia o soporte es "ACTA REUNION".

Fuente: Elaboración ACI

Para 6 de los 15 casos (40%) el soporte diligenciado "Formato de control de cambios" (formato no formalizado), no corresponde a la evidencia definida para la actividad 1 del procedimiento P-TI.06 CONTROL DE CAMBIOS A LA INFRAESTRUCTURA TECNOLÓGICA, cuya evidencia o soporte es "ACTA REUNION".

2.Soporte de aprobación del cambio (actividad 2- Acta de reunión)
De los 15 casos revisados, los casos 1993 y 2097 cuentan con el soporte de aprobación del cambio, y para los 13 (87%) restantes no hay evidencia de la actividad 2, así:

Numero del caso	**Categoría**	Verificación
1675	Red Cableada	Se aportó el ACTA 36 2024-09-26, la cual refiere "A36: Se realizó peinado, maquillado y mantenimiento de los racks del piso 28. Se realiza recorrido el 02/10/2024 9am" Se observó el correo "Cambio peinado rack CCB", que contiene la traza de creación y cierre del caso, pero no se observó la aprobación por el Comité de Cambios

1760	Red Cableada	No existe evidencia “acta de reunión”, de la ejecución de la actividad 2 "Aprobar el cambio ", del procedimiento P-TI.06 CONTROL DE CAMBIOS A LA INFRAESTRUCTURA TECNOLÓGICA
17941	TIQUETES	No existe evidencia “acta de reunión”, de la ejecución de la actividad 2 "Aprobar el cambio ", del procedimiento P-TI.06 CONTROL DE CAMBIOS A LA INFRAESTRUCTU
17981	GEOTEC - FONVIVIENDA	No existe evidencia “acta de reunión”, de la ejecución de la actividad 2 "Aprobar el cambio ", del procedimiento P-TI.06 CONTROL DE CAMBIOS A LA INFRAESTRUCTURA TECNOLÓGICA
2005	Unidades de Almacenamiento	En la trazabilidad del correo aportado, se observó que el cambio fue aprobado viernes, 9 de mayo de 2025 11:28, no obstante, el procedimiento indica que la aprobación es mediante acta de reunión
2012	Servidores Virtuales	No existe evidencia “acta de reunión”, de la ejecución de la actividad 2 "Aprobar el cambio ", del procedimiento P-TI.06 CONTROL DE CAMBIOS A LA INFRAESTRUCTURA TECNOLÓGICA
2019	Servidores Virtuales	Aunque en la descripción del caso se indica que fue aprobado en el acta del 15/05/2025, se observó el acta, y esta actividad se registró como compromiso en la sección "COMPROMISOS ACTA 17 (2025/05/15)", no se observó acta de reunión de la aprobación
2055	Servidores Virtuales	No existe evidencia “acta de reunión”, de la ejecución de la actividad 2 "Aprobar el cambio ", del procedimiento P-TI.06 CONTROL DE CAMBIOS A LA INFRAESTRUCTURA TECNOLÓGICA
2068	Unidades de Almacenamiento	En la trazabilidad del correo aportado, se observó que el cambio fue aprobado 17 de junio de 2025 11:58 a. m., no obstante el procedimiento indica que la aprobación es mediante acta de reunión
2101	Seguridad Perimetral	No existe evidencia “acta de reunión”, de la ejecución de la actividad 2 "Aprobar el cambio ", del procedimiento P-TI.06 CONTROL DE CAMBIOS A LA INFRAESTRUCTURA TECNOLÓGICA
2123	Firewalls	No existe evidencia “acta de reunión”, de la ejecución de la actividad 2 "Aprobar el cambio ", del procedimiento P-TI.06 CONTROL DE CAMBIOS A LA INFRAESTRUCTURA TECNOLÓGICA
2132	Servidores Virtuales	

		No existe evidencia “acta de reunión”, de la ejecución de la actividad 2 "Aprobar el cambio ", del procedimiento P-TI.06 CONTROL DE CAMBIOS A LA INFRAESTRUCTURA TECNOLÓGICA. Uso de 172.16.3.6, para el repositorio solicitado
19905	Sistema Control de asistencia	No existe evidencia “acta de reunión”, de la ejecución de la actividad 2 "Aprobar el cambio ", del procedimiento P-TI.06 CONTROL DE CAMBIOS A LA INFRAESTRUCTURA TECNOLÓGICA

Fuente: Elaboración ACI

Es de anotar que los dos casos de Unidades de Almacenamiento 2005 y 2068, se observó la aprobación mediante correo electrónico, sin embargo, el registro o evidencia definido en el procedimiento para la actividad es “acta de reunión”

3.Anexos de la solicitud en la herramienta de mesa de ayuda

Para los 15 casos 1760, 17941, 17981, 1993, 2005, 2012, 2019, 2055, 2068, 2097, 2101, 2123, y 19905, se observó la creación del caso en la herramienta Aranda y sus anexos.

4. Informe final de ejecución y evidencias de pruebas realizadas. (herramienta de gestión)

De los 15 casos revisados, para 2 (13%) no se observaron los soportes y evidencias de las pruebas realizadas, así:

17941	TIQUETES	En los documentos aportados y en la trazabilidad de correos , no se observó el formato F-TI-22 Pruebas de calidad de software, según P.TI-04 DESARROLLO, MANTENIMIENTO Y PUESTA EN PRODUCCIÓN DE SOFTWARE. Se observó el resultado de las pruebas satisfactorias por parte del usuario. El caso en la herramienta Aranda, según actividad 6 "Cierre de cambio” contiene la imagen del cambio realizado, según correo “Paso a producción tiquetes caso 17941 ajuste límite de informe", que contiene la traza de creación y cierre del caso. 13/11/2024
17981	GEOTEC - FONVIVIENDA	En los documentos aportados y en la trazabilidad de correos , no se observó el formato F-TI-22 Pruebas de calidad de software, según P.TI-04 DESARROLLO, MANTENIMIENTO Y PUESTA EN PRODUCCIÓN DE SOFTWARE. Se socializó el cambio en el acta de cambios N.43 del 14/11/2024, que indica : "A42: APLICATIVO GEOTEC: Se incluyeron nuevos estados, se realizó desarrollo para que dependiendo de la fecha del periodo del reporte que se esté generando se visualice el logo que corresponda (Fonade o Enterritorio), se actualizaron formatos. Previsto el paso a producción el Miércoles 13 de noviembre 2024 a la 1:00 pm " se observó el correo de solicitud paso a producción con el caso 1755

	Frente a esta actividad “Informe final de ejecución” lo observado corresponde a la trazabilidad de la gestión y cierre de cada caso registrada en “Aranda”. Es de anotar, que, en la sesión de trabajo con el operador tecnológico y profesionales de TI del 16/09/2025, indicaron que, de acuerdo con la clasificación del cambio, aplican o no algunos puntos de control, sin embargo, el procedimiento no describe excepciones o casos particulares para la ejecución de las actividades.
CRITERIO:	P-TI-06 CONTROL DE CAMBIOS A LA INFRAESTRUCTURA TECNOLÓGICA v.5 , numeral 6 desarrollo de actividades CTROPETI-36 Procedimientos de control de cambios en la infraestructura tecnológica y mantenimiento de aplicativos en producción
CAUSA PROBABLE:	Omisión en la documentación de los puntos de control definidos en el procedimiento control de cambios de la infraestructura tecnológica
RIESGO	ROPETI-2: Subutilización de las implementaciones de aplicativos en la plataforma tecnológica
CONSECUENCIA:	Desconocer u omitir posibles impactos o riesgos que puedan generar los cambios realizados Falta de trazabilidad de los mantenimientos o actualizaciones realizadas en los componentes tecnológicos
RECOMENDACIÓN(ES):	Dar cumplimiento al procedimiento P-TI-06 CONTROL DE CAMBIOS A LA INFRAESTRUCTURA TECNOLÓGICA v.5, de tal manera que este alineado con la forma de operación, trazabilidad de los cambios en la herramienta de gestión Aranda y soportes definidos para cada actividad. Definir y aplicar una estructura estándar para el “Plan detallado del cambio” y para la recolección de soportes de cada actividad del procedimiento P-TI-06 CONTROL DE CAMBIOS A LA INFRAESTRUCTURA TECNOLÓGICA
NIVEL CRITICIDAD	MODERADO

CONDICIÓN:	Observación 4. Deficiencias en la trazabilidad de atención o trámite de eventos de la plataforma tecnológica Tomando como fuente los informes del operador tecnológico de julio 2024 a julio 2025, en los cuales se describen los monitoreos a la plataforma tecnológica y alertas emitidas por las herramientas implementadas, se seleccionaron los siguientes casos para verificar la trazabilidad y soportes del trámite a los eventos detectados y reportados, así:

Informe operador	Periodo del informe	sección	TIKET / nota del informe
INFORME SERVICIOS DE SEGURIDAD TECNOLÓGICA	27 Julio a 26 Agosto de 2024	5.3 Eventos detectados y gestionados por las herramientas de seguridad- Servicio SOC	81% de los eventos reportados no se obtuvieron retroalimentaciones.
INFORME SERVICIOS DE SEGURIDAD TECNOLÓGICA	27 Julio a 26 Agosto de 2024	5.5 Criticidad 5.6.1 Alertas criticidad Alta	No se recibio feedback
ENTERRITORIO S.A. INFORME MENSUAL NOC	28 agosto a 27 sep 2024	2.6 CASOS ESCALADOS ALTA	TICKET 25472
ENTERRITORIO S.A. INFORME MENSUAL NOC	28 agosto a 27 sep 2024	2.6 CASOS ESCALADOS ALTA	TICKET 25474
INFORME MENSUAL NOC	27-Septiembre al 26- Octubre 2024	2.6 CASOS ESCALADOS	TICKET: 25623
INFORME MENSUAL NOC	27-Septiembre al 26- Octubre 2024	2.6 CASOS ESCALADOS	No registra, 22/10/2024
INFORME MENSUAL NOC	27- Enero al 26 de febrero 2025	2.4 Servicios a nivel de DISCO Ilustración 6. Dispositivos con picos más altos	TICKET 32300

13 May-Jun 2025/2. Seguridad INFORME MENSUAL NOC	27- Mayo al 26 de Junio del 2025	2.3 USO CPU	TICKET 37883
13 May-Jun 2025/2. Seguridad INFORME MENSUAL NOC	27- Mayo al 26 de Junio del 2025	2.3 USO CPU	TICKET 37276
13 May-Jun 2025/2. Seguridad INFORME MENSUAL NOC	27- Mayo al 26 de Junio del 2025	2.3 USO CPU	TICKET 37278
14 Jun-Jul 2025/2. Seguridad INFORME MENSUAL NOC	27- junio al 26 de julio del 2025	2..2 Uso de memoria (RAM)	TICKET 39117
14 Jun-Jul 2025/2. Seguridad INFORME MENSUAL NOC	27- junio al 26 de julio del 2025	2..2 Uso de memoria (RAM)	TICKET 39179

Fuente: Elaboración ACI

Una vez revisados los soportes y respuestas por el proceso Gestión de TI, frente a los casos descritos anteriormente, se estableció una debilidad en el trámite y documentación de las alertas generadas por el Centro de Operaciones de Red-NOC, toda vez que:

Los dos primeros casos, se indicó que son eventos presentados debido al proceso de migración de servicios al nuevo operador, los tickets: 37883, 37278, 39117, 39179, 25474, 25623 y 32300 se indicó que estos eventos obedecen a procesos automáticos ejecutados sobre el servidor a media noche y que no generan afectación en el servicio, que pueden catalogarse como “falsos positivos”, sin embargo, en los informes de gestión mensuales del operador tecnológico se

	registra que fueron debidamente documentadas estas alertas y escaladas mediante los tickets, lo cual genera incertidumbre y falta de precisión frente a lo registrado en dichos documentos.
CRITERIO:	M.RI-06 MANUAL DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN V.6, Numeral 7.20 Gestión del cambio, revisión y monitoreo de los servicios del proveedor, y 7. CONTROLES ORGANIZACIONALES Control CTROPETI-40 Monitoreo a la plataforma tecnológica
CAUSA PROBABLE:	Falta de claridad en la presentación de los resultados del monitoreo a la plataforma tecnológica en los informes mensuales de gestión del operador, en cuanto a la identificación, clasificación y gestión de las alertas generadas el Centro de Operaciones de Red- NOC
RIESGO	ROPETI-10 Hurto de activos de la plataforma tecnológica (información, equipos de cómputo, comunicaciones, procesamiento, audiovisuales, etc.)
CONSECUENCIA:	Posibles eventos o alertas sobre la plataforma tecnológica sin tramite o atención que pueden afectar la disponibilidad de los servicios Información inconsistente en los informes mensuales del operador tecnológico, frente a la gestión de las alertas o eventos generados
RECOMENDACIÓN(ES):	Gestionar integralmente la trazabilidad, documentación y debido registro de los eventos y alertas generadas el Centro de Operaciones de Red- NOC, indicando claramente cuales casos fueron gestionados según criticidad y cuales obedecen a “falsos positivos” Estandarizar la presentación de los resultados de análisis de eventos y alertas detectados por las herramientas de monitoreo en los informes mensuales presentados por el operador tecnológico, y precisar los eventos originados de procesos rutinarios que no requieren ser tramitados y documentados
NIVEL CRITICIDAD	MODERADO

CONDICIÓN:	Observación 5. Inconsistencias en la base de datos persona natural derivada del formato de vinculación de clientes- FVC Una vez realizadas las validaciones de integridad a la base de datos de persona natural generada el 01/09/2025, cuya fuente es el formato de vinculación clientes- formato F-RI-01 – FVC, con 1340 registros para los ID con fecha de diligenciamiento en 2024 y 2025, se identificaron inconsistencias frente a los campos descritos a continuación:

campo validado	ID registro	Resultado
Tipo De Identificación	id 95735 con fecha con Fecha De Diligenciamiento :2024/03/07 id 101506 con Fecha De Diligenciamiento 2025/08/21	En 2 registros tiene este campo =NIT
CELULAR	ID93559, 95728, 96945 y 101320	En 4 registros en número del celular con menos de 10 dígitos.
profesión	Registros 2025:98949, 98874, 83859, 95850, 96297, 92573, 96201, 98172, 100077, 98208, 99244, 98153, 100481,101208, 101107, 98320, 99840, 99814, 100855, 99893, 99516, 99694, 101500, 101538, 99046, 100522, 100226, 100907, 100343 2024: 87367, 95097, 96362, 92513, 92534, 95039, 96520, 96849, 93489, 95436, 95158, 96073, 96602,98026, 97584, 97642, 98271, 98386, 98261, 97843	En 49 registros con el campo "Nivel De Estudios" en posgrado, pero con el campo "profesión" vacío o nulo.
Fuente Bienes Y Recursos	Registros con información inconsistente 2024 y 2025: 97687, 97472, 93852, 95735	En 4 registros el campo "Fuente Bienes Y Recursos" con información incompleta o inconsistente, con datos : "si", 0 , *

Fuente: Elaboración ACI

Resultado de las validaciones anteriores, se establece que 59 de 1340 que representa el 4% de los registros, presentan alguna inconsistencia en los campos registrados en la base de datos persona natural.

CRITERIO:

M.RI-06 MANUAL DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN V.6 numeral 6. Objetivos, Implementar controles enfocados a la protección de la confidencialidad, integridad, disponibilidad de la información.

CAUSA PROBABLE:	Falta de controles automáticos en la captura de datos en el formulario de vinculación de clientes Deficiencias en la definición del control orientado en la calidad de los datos para el SARLAFT
RIESGO	ROPETI-1 Pérdida o falta de integridad de la información almacenada en la plataforma tecnológica y Core del negocio
CONSECUENCIA:	Posibles inconsistencias en la generación de análisis e informes a presentar a Entes de control en el marco de la gestión del SARLAFT
RECOMENDACIÓN(ES):	Implementar reglas de integridad y validación para la captura de datos en el formato de vinculación clientes-FVC en los casos que aplique un control automático según el tipo de dato, para evitar entrada de información inconsistente, Ajustar la definición del control CRLAF63 orientada en realizar validaciones periódicas y aleatorias a la calidad de la información de los diferentes reportes generados para la gestión del SARLAFT
NIVEL CRITICIDAD	Moderado

ANALISIS DE RIESGOS AUDITORÍA

Conclusiones Eficiencia de Control (Diseño)

Es de mencionar que la evaluación del diseño del control se realizó para los controles del mapa de riesgos del proceso Gestión de Tecnologías de la Información**,** según los procedimientos internos objeto del alcance de la auditoría y actividades que por su trascendencia deben considerarse por el proceso como controles.

Se valoraron controles y/ o actividades teniendo en cuenta los siguientes atributos:

Atributos de eficiencia:

- Responsable (Asignado o no asignado)
- Acción (propósito, verbos revisar, verificar, etc.)
- Complemento (Periodicidad, como se realiza, evidencia y desviación)
- Tipo (Preventivo, Detectivo, Correctivo) - Implementación: (Manual o automática)
- Complejidad

Atributos Informativos:

- Documentación (Documentado, sin documentar)
- Frecuencia (Continua, aleatoria)
- Evidencia (Con registro, sin registro)

A continuación, se presentan los resultados obtenidos en cuanto a la evaluación del diseño de controles:

RIESGO	DESCRIPCIÓN CONTROL	IMPLEMENTACIÓN		TIPO		FRECUENCIA		DOCUMENTACIÓN		EVIDENCIA		COMPLEJIDAD		CALIFICACIÓN EFICIENCIA DEL DISEÑO DE CONTROL		CONCLUSIONES/RECOMENDACIONES CONTROL
ROPETI-2 Pérdidas económicas por gastos para la Sociedad por ajustes y nuevas implementaciones tecnológicas a proveedores de aplicativos y/o impacto operativo por reprocesos, deficiencias en las funcionalidades o la subutilización de las implementaciones de aplicativos en la plataforma tecnológica	**CTROPETI-27** Definición de requerimientos a aplicativos Cada vez que se requiera implementar un aplicativo nuevo, El Grupo de Tecnologías de la Información en conjunto con el Grupo de Trabajo usuario, identifica los requerimientos técnicos, funcionales y seguridad de la aplicación a implementar. Con base en este análisis, se establece si el aplicativo será adquirido o desarrollado internamente.	Manual	0,15	Preventivo	0,3	Continuo	0,2	Documentado	0,05	Registro material	0,1	Alta	0,03	78%	Bueno	Recomendación1: Revisar y ajustar el objetivo del control, ya que no está alineado con la descripción del control, toda vez que el control refiere a determinar " si el aplicativo será adquirido o desarrollado internamente. " y el objetivo del control refiere al correcto funcionamiento de los nuevos aplicativos Recomendación2: Incluir en el procedimiento P-TI-04_V05 Desarrollo, mantenimiento y puesta en producción de software, en las condiciones generales o en las primeras actividades, lo referente al estudio de viabilidad del desarrollo solicitado. Recomendación3: Analizar e incluir en la definición del riesgo, la causa referente a deficiencias en el análisis técnico de los requerimientos que puede conllevar a elegir la opción menos favorable en relación costos/beneficios
	CTROPETI-36 Procedimientos de control de cambios en la infraestructura tecnológica y mantenimiento de aplicativos en producción La Sociedad cuenta con el procedimiento de control de cambios en la infraestructura tecnológica los cuales son administrados por el Grupo de Tecnologías de la Información, teniendo en cuenta el impacto que puede causar sobre los demás elementos y en los servicios soportados. Adicionalmente, se cuenta con una metodología para el mantenimiento de aplicativos que se encuentran en producción, por medio de la cual, según la naturaleza del cambio presentado o por evento, se analiza el impacto y su afectación en estructuras de bases de datos o código, y se determina su viabilidad. (Adquisición, desarrollo y puesta en producción de software). El líder funcional por evento registra su descripción y anexos de la solicitud en la herramienta de mesa de ayuda o mediante correo electrónico a la mesa de ayuda. El Grupo de Tecnologías de	Manual	0,15	Preventivo	0,3	Continuo	0,2	Documentado	0,05	Registro Sustancial	0,1	Alta	0,03	83%	Excelente	Recomendación 1: incluir la periodicidad "semanal" de los comités de cambios como están programados, en el procedimiento P-TI-06_V05 Control de cambios a la infraestructura tecnológica. Verificar y ajustar la descripción del control que incluya una acción orientada en revisar, validar, cotejar, comparar, aprobar, entre otras. Recomendación 2: Separar el control, uno para cambios a componentes tecnológicos y otro para mantenimiento de aplicativos en producción, que ya se encuentra documentado en el control CTROPETI-3

	la Información y el Operador mediante correo electrónico notifican a los responsables de las pruebas para validar la correcta implementación del cambio y se documenta en el informe final las evidencias de las pruebas para posterior cierre del caso.															
ROPETI-4 Impacto operacional para los procesos de la Sociedad, debido a la inoportunidad en la atención de requerimientos de actualización, desarrollo, mejora a los sistemas de información o soporte tecnológico	**CTROPETI-12** Metodología estándar para el desarrollo y/o mantenimiento de aplicativos Los Grupos de Trabajo y Líderes Funcionales realizan requerimientos a través de la Mesa de Ayuda y aplicativo ARANDA dando cumplimiento al procedimiento Desarrollo, mantenimiento P-TI-04. Una vez evaluadas las necesidades por parte del líder de desarrollo se dará inicio a la solución en caso de ser viable.	Manual	0,15	Preventivo	0,3	Continuo	0,2	Documentado	0,05	Registro Sustancial	0,1	Media	0,07	87%	Excelente	Recomendación: Revisar y ajustar la defi control, teniendo en cuenta que la escenc " evaluar las necesidades por parte de líc y dar inicio a la solución en caso de ser vi solicitudes de los usuarios como inicia la control.
	CTROPETI-3 Mantenimiento de aplicaciones El Líder de Sistemas de Información según demanda, se encarga de atender de forma controlada y organizada las necesidades de soporte y ajuste a las aplicaciones de la Sociedad, direccionando las solicitudes de mantenimiento a los ingenieros responsables.	Manual	0,15	Preventivo	0,3	Continuo	0,2	Documentado	0,05	Registro material	0,1	Media	0,07	82%	Excelente	Recomendación1: Evaluar la pertinencia control CTROPETI-3 (Metodología estánc desarrollo y/o mantenimiento de aplicativo CTROPETI-12 (Mantenimiento de aplicati en cuenta que estan orientados en analiz requerimientos de nuevas funcionalidades ajustes a los aplicativos existentes, y apli procedimiento P-TI-04_V05 Desarrollo, n puesta en producción de software, y la gu Desarrollo, ajuste y estandarización de sc Recomendación 2 incluir el N. del caso Ar archivo Excel que diligencia el lider de de asignación y seguimiento de los casos a ingenieros
ROPETI-9 Multas y/o sanciones por incumplimientos en la trasmisión de información a entes de vigilancia y control, Impacto operativo por la interrupción de operaciones tecnológicas y deterioro de la imagen de la Sociedad por comentarios negativos en redes sociales y similares debido al daño o malfuncionamiento	**CTROPETI-12** Metodología estándar para el desarrollo y/o mantenimiento de aplicativos Los Grupos de Trabajo y Líderes Funcionales realizan requerimientos a través de la Mesa de Ayuda y aplicativo ARANDA dando cumplimiento al procedimiento Desarrollo, mantenimiento P-TI-04. Una vez evaluadas las necesidades por parte del líder de desarrollo se dará inicio a la solución en caso de ser viable.	Manual	0,15	Preventivo	0,3	Continuo	0,2	Documentado	0,05	Registro Sustancial	0,1	Media	0,07	87%	Excelente	Recomendación: Revisar y ajustar la defi control, teniendo en cuenta que la escenc " evaluar las necesidades por parte de líc y dar inicio a la solución en caso de ser vi solicitudes de los usuarios como inicia la control.

del hardware o software																
ROPETI-10 Pérdida de activos (hardware e información), o impacto operativo por reprocesos para recuperación de información, o deterioro de la imagen de la Sociedad por reclamaciones de terceros, debido al hurto de activos de la plataforma tecnológica (información, equipos de cómputo, comunicaciones, procesamiento, equipos audiovisuales, etc.)	**CTROPETI-23** Control de acceso físico a los cuartos de comunicaciones El Grupo de Tecnologías de la Información controla y autoriza el ingreso a los centros de cableado de cada piso que se encuentra restringido. En algunos centros de cableado que se encuentran dentro de oficinas con acceso restringido para el ingreso a estas, se solicita autorización a Servicios Administrativos. Por su parte Servicios Administrativos tiene una copia de las llaves de los centros de cableado.	Manual	0,15	Preventivo	0,3	Continuo	0,2	Documentado	0,05	Registro material	0,1	Baja	0,1	85%	Excelente	Recomendación1: Implementar el diligenc planilla de ingreso para todos los centros comunicaciones adicional al piso 28. Recomendación2: Revisar y ajustar la des control mencionando el registro de ingres y puntualizar los pisos que cuentan con c cableado que requieren el control de ingr en cuenta que el control indica "En alguno cableado (...) ". A su vez definir los perfile autorizados de ingreso a estos espacios Recomendación3: Actualizar el atributo "DOCUMENTACIÓN" en el control SIAR, MANUAL DE POLÍTICAS DE SEGURIDA INFORMACIÓN v.6 , 9.1 Perímetro de se
	CTROPETI-40 Monitoreo a la plataforma tecnológica El Operador Tecnológico por evento realiza el monitoreo a la plataforma tecnológica, con el fin de generar alertas tempranas a las potenciales fallas en los dispositivos tecnológicos. En caso de generarse alarmas el Líder de Infraestructura del Grupo de Tecnologías de la Información realiza seguimiento a las mismas y solicita los ajustes necesarios.	Automatizado	0,25	Preventivo	0,3	Continuo	0,2	Documentado	0,05	Registro Sustancial	0,1	Media	0,07	97%	Excelente	Recomendación 1: Analizar e incluir en la riesgo, la causa referente a ocurrencia de anomalos o de seguridad de la informació oportunamente, que pueden generar perc información Recomendación2: Complementar la docu control con el contrato del operador tecno TÉCNICO No. 2 – SERVICIOS DE SEGU TECNOLÓGICA" , y la politica del manua de la información M-RI-06 Recomendación3: Revisar y ajustar el car , ya que se observó que el registro esta c matriz SIAR como material, sin embargo, registro sustancial (logs y alertas) ; a su v soportes, complementar con los informes tecnológico donde se presentan los analis eventos detectados por periodo.

RIESGO	CONTROL	FORMA DE EJECUCIÓN		TIPO DE CONTROL		APLICACIÓN DEL CONTROL		SOPORTE		COMPLEJIDAD		DOCUMENTACIÓN		RESULTADO DISEÑO DE CONTROL		CONCLUSIONES/RECOMENDACIONES DISEÑO DE CONTROL
R14 Posible identificación inadecuada de riesgos de lavado de activos y financiación del terrorismo, debido a la falta de análisis sobre el comportamiento del mercado en las diferentes líneas del negocio	**CRLAF63** La Gerencia de Tecnologías de la Información realizará semestralmente un informe de actividades realizadas con el fin de mejorar la calidad de los datos. Lo anterior a partir de las inconsistencias que son reportadas por correo y reportará por correo electrónico a los responsables de registro de la información en los distintos aplicativos dispuestos por la entidad, para que se ajusten las novedades identificadas en el mismo informe, de tal forma que se disponga de información actualizada, que cumpla con características tales como: Oportunidad, completitud, unicidad/singularidad, validez, consistencia y Exactitud.	Manual/Visual	0,08	Correctivo	0,07	Periódico	0,23	Se generan y se conservan	0,05	Media	0,07	Sin documentar	0	50%	Moderada	**Recomendación1**: Revisar y ajustar la descripción del control, toda vez que "realizar un informe " es una actividad. Un control debe contener una acción orientada en revisar, validar, cotejar, comparar, ajustar si es correctivo, entre otras. **Recomendación2:** como actividad complementaria al control, realizar jornadas de sensibilización a los usuarios en el uso de los aplicativos y la importancia que los datos de entrada sean oportunos y de calidad
	CRLAF64 La Gerencia de Tecnologías de la Información en mesas de trabajo con el Grupo de cumplimiento SARLAFT realizaran mensualmente acciones que permitan verificar que los desarrollos solicitados por el Grupo Cumplimiento SARLAFT, con el fin, de que se encuentran actualizados y operando correctamente cada uno de los requerimientos acordados.	Manual/Visual	0,08	Preventivo	0,2	Periódico	0,23	Se generan y se conservan	0,05	Media	0,07	Sin documentar	0	63%	Bueno	Estos dos controles a cargo de TI permiten gestionar los requerimientos de nuevas funcionalidades y/o mantenimientos a los aplicativos y/o reportes fuentes para la gestión del SARLAFT. Se incluye en las pruebas de auditoria

Consolidado del Diseño de Controles

IMPLEMENTACIÓN		TIPO		FRECUENCIA		DOCUMENTACIÓN		EVIDENCIA		COMPLEJIDAD		CALIFICACIÓN EFICIENCIA DEL DISEÑO DE CONTROL	
Manual	6	Preventivo	7	Continuo	7	Documentado	7	Registro material	3	Alta	2	Excelente	6
Automatizado	1	Detectivo	0	Aleatorio	0	sin documentar	0	Registro Sustancial	4	media	4	Bueno	1
		Correctivo	0							baja	1		

Conclusiones Efectividad de Control
La efectividad de los controles de la matriz de riesgos SIAR se realizó de acuerdo con la respuesta a las siguientes preguntas por criterio:

Efectividad del control
1. Cumple con el objetivo de control. ¿Las actividades que se desarrollan buscan por si solas prevenir o detectar las causas originadoras
2. ¿La persona que aplica el control tiene la autoridad y/o competencias para ello?
3. ¿El responsable de aplicar el control conoce los efectos que implican su omisión?
4. ¿Existen mecanismos para identificar la no aplicación o desviación en el control?
5. ¿Las observaciones, desviaciones o diferencias identificadas durante la ejecución del control son investigadas y resueltas oportunamente?
6. ¿El control opera tal y como fue diseñado, de acuerdo con sus atributos?
7. ¿La fuente de información utilizada en la ejecución del control es confiable?
8. ¿El control contribuye a mitigar la causa o la consecuencia?

Omisión en la aplicación

9. Afectar la información contable y los estados financieros
10. Generar posible deterioro de la imagen y/o reputación de la entidad
11. Genera responsabilidad Administrativa
12. En el último año se han presentado eventos de riesgo por la omisión del control
13. Generar posibles pérdidas económicas

DESCRIPCIÓN RIESGO	CONTROL	RESULTADO	RESULTADO OMISION	RESULTADO COBERTURA	Observaciones
ROPETI-2 Pérdidas económicas por gastos para la Sociedad por ajustes y nuevas implementaciones tecnológicas a proveedores de aplicativos y/o impacto operativo por reprocesos, deficiencias en las funcionalidades o la subutilización de las	**CTROPETI-27** Definición de requerimientos a aplicativos Cada vez que se requiera implementar un aplicativo nuevo, El Grupo de Tecnologías de la Información en conjunto con el Grupo de Trabajo usuario, identifica los requerimientos técnicos, funcionales y seguridad de la aplicación a implementar. Con base en este análisis, se establece si el aplicativo será adquirido o desarrollado internamente.	85%	65%	77%	

implementaciones de aplicativos en la plataforma tecnológica	**CTROPETI-36** Procedimientos de control de cambios en la infraestructura tecnológica y mantenimiento de aplicativos en producción La Sociedad cuenta con el procedimiento de control de cambios en la infraestructura tecnológica los cuales son administrados por el Grupo de Tecnologías de la Información, teniendo en cuenta el impacto que puede causar sobre los demás elementos y en los servicios soportados. Adicionalmente, se cuenta con una metodología para el mantenimiento de aplicativos que se encuentran en producción, por medio de la cual, según la naturaleza del cambio presentado o por evento, se analiza el impacto y su afectación en estructuras de bases de datos o código, y se determina su viabilidad. (Adquisición, desarrollo y puesta en producción de software). El líder funcional por evento registra su descripción y anexos de la solicitud en la herramienta de mesa de ayuda o mediante correo electrónico a la mesa de ayuda. El Grupo de Tecnologías de la Información y el Operador mediante correo electrónico notifican a los responsables de las pruebas para validar la correcta implementación del cambio y se documenta en el informe final las evidencias de las pruebas para posterior cierre del caso.	85%	0,6	75%	Observación 3. Deficiencias en el registro y seguimiento al control de cambios de los componentes tecnológicos	
ROPETI-4 Impacto operacional para los procesos de la Sociedad, debido a la inoportunidad en la atención de requerimientos de actualización, desarrollo, mejora a los sistemas de información o soporte tecnológico	**CTROPETI-12** Metodología estándar para el desarrollo y/o mantenimiento de aplicativos Los Grupos de Trabajo y Líderes Funcionales realizan requerimientos a través de la Mesa de Ayuda y aplicativo ARANDA dando cumplimiento al procedimiento Desarrollo, mantenimiento P-TI-04. Una vez evaluadas las necesidades por parte del líder de desarrollo se dará inicio a la solución en caso de ser viable.	85%	65%	77%	Observación 02. Deficiencias en la trazabilidad y registro del ciclo de desarrollo de software	
	CTROPETI-3 Mantenimiento de aplicaciones El Líder de Sistemas de Información según demanda, se encarga de atender de forma controlada y organizada las necesidades de soporte y ajuste a las aplicaciones de la Sociedad, direccionando las solicitudes de mantenimiento a los ingenieros responsables.	85%	85%	85%		
ROPETI-9 Multas y/o sanciones por incumplimientos en la trasmisión de información a entes de vigilancia y control, Impacto operativo por la interrupción de operaciones tecnológicas y deterioro de la imagen de la Sociedad por comentarios negativos en redes sociales y similares debido al daño o malfuncionamiento del hardware o software	**CTROPETI-12** Metodología estándar para el desarrollo y/o mantenimiento de aplicativos Los Grupos de Trabajo y Líderes Funcionales realizan requerimientos a través de la Mesa de Ayuda y aplicativo ARANDA dando cumplimiento al procedimiento Desarrollo, mantenimiento P-TI-04. Una vez evaluadas las necesidades por parte del líder de desarrollo se dará inicio a la solución en caso de ser viable.	85%	65%	77%		

ROPETI-10 Pérdida de activos (hardware e información), o impacto operativo por reprocesos para recuperación de información, o deterioro de la imagen de la Sociedad por reclamaciones de terceros, debido al hurto de activos de la plataforma tecnológica (información, equipos de cómputo, comunicaciones, procesamiento, equipos audiovisuales, etc.)	**CTROPETI-23** Control de acceso físico a los cuartos de comunicaciones El Grupo de Tecnologías de la Información controla y autoriza el ingreso a los centros de cableado de cada piso que se encuentra restringido. En algunos centros de cableado que se encuentran dentro de oficinas con acceso restringido para el ingreso a estas, se solicita autorización a Servicios Administrativos. Por su parte Servicios Administrativos tiene una copia de las llaves de los centros de cableado.	100%	65%	86%	
	CTROPETI-40 Monitoreo a la plataforma tecnológica El Operador Tecnológico por evento realiza el monitoreo a la plataforma tecnológica, con el fin de generar alertas tempranas a las potenciales fallas en los dispositivos tecnológicos. En caso de generarse alarmas el Líder de Infraestructura del Grupo de Tecnologías de la Información realiza seguimiento a las mismas y solicita los ajustes necesarios.	85%	60%	85%	Observación 4. Deficiencias en la trazabilidad de atención o trámite de eventos de la plataforma tecnológica

CONTROL	RESULTADO	RESULTADO OMISION	conclusiones
CTROPETI-27	85%	65%	Resultado 85%: El control es preventivo debido a que contribuye a mitigar la causa del riesgo, referente a inconsistencias en los requerimientos definidos por parte de los usuarios y la valoración técnica por parte del Grupo de Tecnología de la Información, el registro y seguimiento se lleva en la herramienta de gestión Aranda. No obstante, no opera como está definido porque hay deficiencias en la trazabilidad y registro documental del ciclo de desarrollo de software, según G-TI-02 DESARROLLO, AJUSTE Y ESTANDARIZACIÓN DE SOFTWARE Resultado omisión 65%: puede generar responsabilidad Administrativa para los profesionales de TI, y posibles pérdidas económicas, por desarrollar o adquirir aplicativos que no cumplan con las especificaciones técnicas y/o funcionales requeridas por el usuario, y/o costos de horas de desarrollo por reprocesos

CTROPETI-36	85%	60%	Resultado 85%: El control es preventivo porque cambios a realizar en algún componente tecnológico requieren de análisis integral, pruebas, aprobación e implementación del cambio según aplique, mediante comité de cambios semanal realizado por el operador tecnológico y profesionales de TI, el registro y documentación se realiza en la herramienta Aranda. Sin embargo, no opera como está definido porque se identificaron deficiencias en el registro y trazabilidad documental de las actividades descritas en el procedimiento P.TI-06 CONTROL DE CAMBIOS A LA INFRAESTRUCTURA TECNOLÓGICAResultado omisión 60%: puede generar responsabilidad Administrativa para los profesionales de TI, y afectar la imagen de la Sociedad por posible indisponibilidad de componentes tecnológicos, como la página WEB institucional, derivado de cambios que no surtieron el análisis integral de riesgos o impactos
CTROPETI-12	85%	65%	Resultado 85%: El control es preventivo debido a que contribuye a mitigar la causa del riesgo, referente a inconsistencias en los requerimientos definidos por parte de los usuarios y la valoración técnica por parte del Grupo de Tecnología de la Información, el registro y seguimiento se lleva en la herramienta de gestión Aranda. No obstante, no opera como esta definido porque hay deficiencias en la trazabilidad y registro documental del ciclo de desarrollo de software, según G-TI-02 DESARROLLO, AJUSTE Y ESTANDARIZACIÓN DE SOFTWARE Resultado omisión 65%: puede generar responsabilidad Administrativa para los profesionales de TI, generar posibles pérdidas económicas, por desarrollar o adquirir aplicativos que no cumplan con las especificaciones técnicas y/o funcionales requeridas por el usuario, y/o costos de horas de desarrollo por reprocesos
CTROPETI-3	85%	85%	Resultado 85%: El control es preventivo debido a los análisis y procedimiento definidos para el mantenimiento de aplicativos en producción, por parte del equipo de desarrollo. Sin embargo, no opera como esta definido, con sustento en que en dos casos revisados (17981 y 19905) no cuentan con la documentación soporte de las actividades según procedimiento P.TI-06 CONTROL DE CAMBIOS A LA INFRAESTRUCTURA TECNOLÓGICA Resultado omisión 85%: puede generar responsabilidad Administrativa para los profesionales de TI
CTROPETI-23	100%	65%	Resultado 100%: El control es preventivo porque restringe el acceso de personal no autorizado al datacenter del piso 28 y a los rack de comunicaciones de los pisos. Resultado omisión 65%: puede generar responsabilidad Administrativa para los profesionales de TI, y posibles perdidas económicas por perdida o daños de los componentes del centro de computo o del rack de comunicaciones
CTROPETI-40	85%	60%	Resultado 85%: el control es preventivo debido a que con las herramientas de monitoreo permanentes a la plataforma tecnológica, se detectan y gestionan los eventos o alertas que puedan afectar los servicios tecnológicos, en el marco de las obligaciones del operador tecnológico. Sin embargo, no opera como esta diseñado porque se identificaron inconsistencias en la información, análisis y documentación de algunos tikes descritos en los informes mensuales de gestión Resultado omisión 60%: puede generar responsabilidad Administrativa para el supervisor del contrato del OT, y afectar la reputación de la Sociedad, por indisponibilidad de los servicios tecnológicos al no gestiona adecuadamente los eventos o alertas detectadas

Riesgos analizados del proceso o unidad auditable

1.ROPETI-2: Subutilización de las implementaciones de aplicativos en la plataforma tecnológica

2. ROPETI-4 Inoportunidad en la atención de requerimientos de actualización, desarrollo, mejora a los

3.ROPETI-9 Daño o malfuncionamiento del hardware o software

4.ROPETI-10: Hurto de activos de la plataforma tecnológica (información, equipos de cómputo, comunicaciones, procesamiento, audiovisuales, etc.)

5. ROPETI-9 Daño o malfuncionamiento del hardware o software

6.R14 Posible identificación inadecuada de riesgos de lavado de activos y financiación del terrorismo, debido a la falta de análisis sobre el comportamiento del mercado en las diferentes líneas del negocio

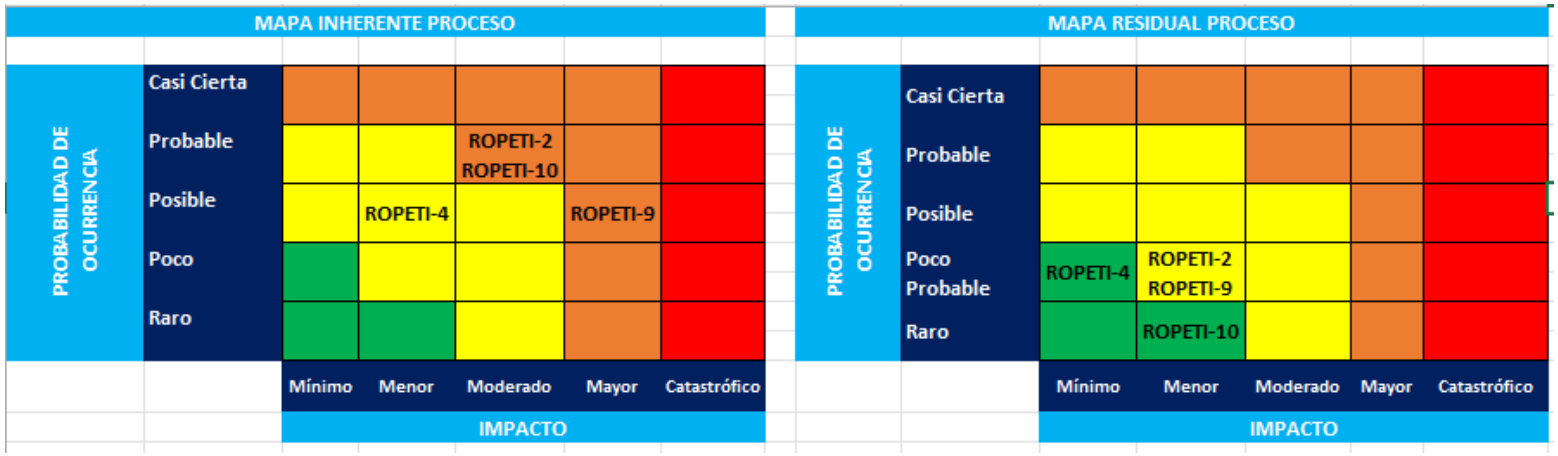
Riesgos emergentes

No se identificaron durante la ejecución de la auditoria

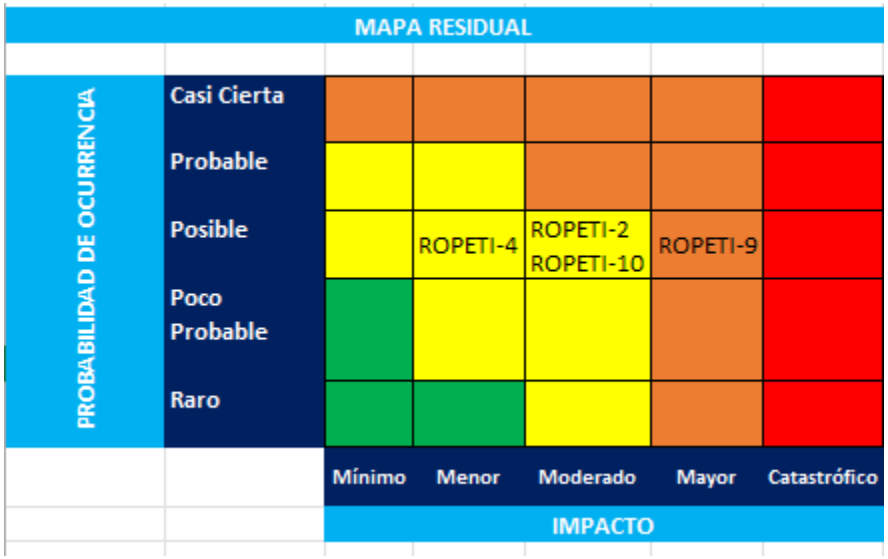
Eventos de riesgo identificados en el ejercicio auditor:

A partir del ejercicio de auditoría realizado al proceso de Gestión de Tecnologías de la información centrado en el análisis y evaluación de riesgos y controles, se evidenciaron los eventos de riesgo descritos en las observaciones.

1) **COMPARATIVO DEL MAPA DE CALOR RIESGO RESIDUAL "PROCESO" VS. "AUDITORÍA"**



MAPA DE CALOR DESPUES DE LA AUDITORÍA



Riesgo	zona residual proceso	zona residual auditoria	Situaciones identificadas
ROPETI-2 Subutilización de las implementaciones de aplicativos en la plataforma tecnológica	MODERADO	MODERADO	En el ejercicio auditor se identificó un evento de riesgo, y producto de esto en el informe de auditoría se registró la observación 3 referente a Deficiencias en el registro y seguimiento al control de cambios de los componentes tecnológicos
ROPETI-4 Inoportunidad en la atención de requerimientos de actualización, desarrollo, mejora a los sistemas de información o soporte tecnológico	BAJO	MODERADO	En el ejercicio auditor se identificó un evento de riesgo, y producto de esto en el informe de auditoría se registró la observación 2 referente a Deficiencias en la trazabilidad y registro del ciclo de desarrollo de software, en relación con el control CTROPETI-12, asociado a estos dos riesgos Este evento genera el desplazamiento de la zona residual de los riesgos
ROPETI-9 Daño o malfuncionamiento del hardware o software	MODERADO	CONSIDERABLE	

ROPETI-10 Hurto de activos de la plataforma tecnológica (información, equipos de cómputo, comunicaciones, procesamiento, audiovisuales, etc.)	BAJO	MODERADO	En desplazamiento en el nivel de riesgo residual, obedece a que en el ejercicio auditor se identificó un evento de riesgo, y producto de esto en el informe de auditoría se registró la observación 4 referente a Deficiencias en la trazabilidad de atención o trámite de eventos de la plataforma tecnológica. En cuanto al control de acceso físico al datacenter y cuartos de comunicaciones se estableció que la efectividad es buena

RECOMENDACIONES RESPECTO DEL ANÁLISIS DE RIESGOS Y CONTROLES DEL PROCESO

Revisar y ajustar la definición de los controles y sus objetivos, de tal forma que cumplan con las características de un control, esto implica considerar la claridad del propósito del control (verificar, validar, cotejar, conciliar, etc.), a su vez ajustar los atributos del diseño según corresponda en concordancia con los procedimientos vigentes y soportes de ejecución de las actividades.

Frente a los eventos de riesgos materializados

ROPETI-2: Dar cumplimiento al procedimiento P-TI-06 CONTROL DE CAMBIOS A LA INFRAESTRUCTURA TECNOLÓGICA v.5, de tal manera que este alineado con la forma de operación, trazabilidad de los cambios en la herramienta de gestión Aranda y con los soportes definidos para cada actividad.

Definir y aplicar una estructura estándar para el “Plan detallado del cambio” y para la recolección de soportes de cada actividad del procedimiento P-TI-06 CONTROL DE CAMBIOS A LA INFRAESTRUCTURA TECNOLÓGICA

ROPETI-4: y ROPETI-9: Documentar los casos de desarrollo de acuerdo con la guía G-TI-02 DESARROLLO, AJUSTE Y ESTANDARIZACIÓN DE SOFTWARE para cada fase tomando en consideración los numerales “*Tareas a realizar”* y *“productos a obtener”* , estandarizando su identificación y soportes definitivos validados en su integridad y completitud, que den cuenta del cumplimiento de cada ítem.

Verificar las condiciones generales de la guía G-TI-02 DESARROLLO, AJUSTE Y ESTANDARIZACIÓN DE SOFTWARE y del procedimiento P-TI-04_V05 Desarrollo, mantenimiento y puesta en producción de software, a fin de establecer los lineamientos para aquellos casos que no le apliquen las reglas generales, o tengan un tratamiento particular.

ROPETI-10: Gestionar integralmente la trazabilidad, documentación y debido registro de los eventos y alertas generadas el Centro de Operaciones de Red- NOC, indicando claramente cuales casos fueron gestionados según criticidad y cuales obedecen a “falsos positivos”

Estandarizar la presentación de los resultados de análisis de eventos y alertas detectados por las herramientas de monitoreo en los informes mensuales presentados por el operador tecnológico, y precisar los eventos originados de procesos rutinarios que no requieren ser tramitados y documentados

CRLAF63: Revisar y ajustar la descripción y atributos del control, toda vez que “realizar un informe " es una actividad. Un control debe contener una acción orientada en revisar, validar, cotejar, comparar, ajustar si es correctivo, entre otras.

FIRMA DEL INFORME DE AUDITORÍA:		
FECHA DE APROBACIÓN:		
NOMBRE	**RESPONSABILIDAD**	**FIRMA**
Orlando Correa Nuñez	Jefe Oficina de Control Interno	
Celeny González Parra	Auditor Líder