

 Agencia de Renovación del Territorio	INFORME	Código: FM-SEM-08
	SEGUIMIENTO EVALUACIÓN Y MEJORA	Versión: 05
	Grupo Interno de Trabajo de Control Interno	Publicado. 28-06-2024

N° DE INFORME	4.3.1
TIPO DE INFORME	Evaluación de los riesgos y controles de Tecnologías de la Información TI y Seguridad de la Información SI
PROCESO	CP-TI-03. V1 Proceso Tecnologías de la Información
RESPONSABLES	Jefe Oficina de Tecnologías de la Información
EQUIPO AUDITOR	
Marisol Gutierrez Hernández	
1. OBJETIVO GENERAL	
Evaluar el diseño y ejecución de los controles establecidos para la gestión de los riesgos identificados en la Matriz de Riesgos de Seguridad de la Información y en la Matriz de Riesgos del Proceso de TI, así como las acciones definidas en los planes de tratamiento y su respectivo seguimiento.	
2. OBJETIVOS ESPECÍFICOS	
1. Evaluar el diseño y ejecución de los controles a partir de los criterios definidos en la Guía para la Gestión Integral del Riesgo en Entidades Públicas y a partir de ello determinar si son adecuados para evitar la materialización de riesgos¹. 2. Verificar que se realice seguimiento a la ejecución de los controles y acciones del plan de manejo de riesgos y que los mismos estén soportados en evidencias².	
3. ALCANCE	
La evaluación tiene como alcance la revisión de controles del Mapa de Riesgos de Seguridad de la Información así como el Mapa de Riesgos del proceso de Tecnología de la información de la vigencia 2026 con corte al 30 de julio.	
4. CRITERIOS (NORMATIVIDAD)	
• Ley 87 de 1993, artículo 12. Funciones de los auditores internos. c) <i>Verificar que los controles definidos para los procesos y actividades de la organización, se cumplan por los responsables de su ejecución y en especial, que las áreas o empleados encargados de la aplicación del régimen disciplinario ejerzan adecuadamente esta función;</i> d) <i>Verificar que los controles asociados con todas y cada una de las actividades de la organización estén adecuadamente definidos, sean apropiados y se mejoren permanentemente, de acuerdo con la evolución de la entidad;</i> g. <i>Verificar los procesos relacionados con el manejo de los recursos, bienes y los sistemas de información de la entidad y recomendar los correctivos que sean necesarios.</i> • Decreto 648 de 2017, artículo 2.2.21.3.1. <i>“El Sistema Institucional de Control Interno estará integrado por el esquema de controles de la organización, la gestión de riesgos, la administración de la información y de los recursos y por el conjunto de planes, métodos, principios, normas, procedimientos, y mecanismos de verificación y evaluación adoptados por la entidad, dentro de las políticas trazadas por la dirección y en atención a las metas, resultados u objetivos de la entidad.”</i> • Guía Rol de las Unidades de Control Interno, Auditoría Interna o quien haga sus veces. DAFP. 2023. • Guía para la Gestión Integral del Riesgo en Entidades Públicas. Versión 7. DAFP 2025. Capítulo V, Numerales: 5.8 Estructura para la Descripción del Control, 5.9 Valoración de Controles • MI-TI-01-V5 Manual de Políticas de Seguridad de la Información Numeral 6. POLÍTICAS ORGANIZACIONALES -6.1. ROLES Y RESPONSABILIDADES. Responsable de Seguridad de la Información <i>“Liderar la gestión de activos, riesgos de seguridad digital y de la información, teniendo en cuenta las metodologías establecidas por la Entidad y a nivel normativo, desde la identificación, análisis, valoración y definición de los planes de tratamiento en la Entidad”.</i> • POL-DE-08 V1 Manual de Política de Administración del Riesgo 2024. Numeral 9.1. Monitoreo de los riesgos y controles. 9.2 Seguimiento a los mapas de riesgos.	

¹ Manual Operativo MIPG V62026. Pag 152 “Verificación del diseño y ejecución de los controles que mitigan los riesgos estratégicos o institucionales.”

 Agencia de Renovación del Territorio	INFORME	Código: FM-SEM-08
	SEGUIMIENTO EVALUACIÓN Y MEJORA	Versión: 05
	Grupo Interno de Trabajo de Control Interno	Publicado. 28-06-2024

- Mapa de Riesgos de Seguridad de la Información ART 2026 FM-TI-36 V2 Formato Instrumento Mapa de Riesgos, Controles y Plan de Acción SI; Mapa de Riesgos del Proceso de TI Formato FM-DE-18

5. PERSONAL ENTREVISTADO

Delegados OTI: Juan José Sánchez Rodríguez, Deysi Viviana Gómez; John Freyder Reyes Castaneda Henry Armando Fernández Miranda.

6. METODOLOGÍA

Se informó mediante Memorando 20261010053703 del 05 de agosto del 2026 a la OTI, la ejecución del informe correspondiente a la evaluación de riesgos y controles de Seguridad de la Información vigencia 2026; En reuniones programadas con los delegados, se revisaron generalidades de: la Matriz de riesgos de Seguridad de la Información vigente, Matriz de Riesgos de TI y el Seguimiento a las acciones correspondientes al Plan de Manejo de Riesgos de Seguridad de la Información.

De la matriz de riesgos de Seguridad de la Información, se establecieron 87 riesgos y 99 controles para los 33 activos de información identificados; se evaluaron 51 controles (es decir una muestra del 51%) y se revisaron las evidencias correspondientes que fueron aportadas en el repositorio de OneDrive de la OTI al cual se dio acceso (enlace: [Seguimiento 2026 Riesgos SI](#)).

Respecto de los riesgos del proceso de Tecnología de la Información, se evaluaron los 8 controles establecidos en la matriz institucional para los 4 riesgos identificados.

Se aplicaron los criterios y metodología para evaluar el diseño y ejecución de los controles del papel de trabajo establecido por el GIT de Control Interno con base en los lineamientos del DAFP así:

Tabla N°1:

³ Criterio por evaluar	Factor por evaluar	Puntaje	Puntaje Total
Asignación y segregación del responsable	Responsable asignado	10	15
	Existe segregación en las actividades de control	5	
	No se identifica responsable	0	
Periodicidad o Frecuencia ⁴	Se describe la periodicidad y en la ejecución es Oportuna y continua	15	15
	Se ejecuta, pero no es claro cuando	10	
	No describe periodicidad.	0	
Propósito ⁵ – Acción de la Actividad de Control	Se describe la acción de acuerdo con un verbo indicativo de control y de acuerdo con lo determinado (Preventivo o Detectivo). Se observa el propósito, pero tiene debilidades en su redacción .	15	15
	No es un control /No se observa propósito: No es claro, corresponde a actividades, pero no de control, de acuerdo con el verbo utilizado o actividad desarrollada	10	
		0	

2 Manual Operativo MIPG V62026. Pag 152 "Verificación de que los responsables estén ejecutando los controles tal como han sido diseñados."

3 Aspectos por evaluar dentro del Sistema de Control Interno - Manual Operativo MIPG V6-2026. Pág. 151 "Verificación de que el diseño del control establecido por la primera línea de defensa sea pertinente frente a los riesgos identificados, analizando: los responsables y su adecuada segregación de funciones, propósito, periodicidad, tratamiento en caso de desviaciones, forma de ejecutar el control y evidencias de su ejecución, y efectuar las recomendaciones a que haya lugar ante las instancias correspondientes (primera, segunda, y línea estratégica)."

4 Corresponde a la periodicidad con la cual se ejecuta una actividad de control debe ser adecuada para detectar o prevenir el riesgo en función de su nivel de exposición inherente. (puede ser periódica o por evento). Guía para la Gestión Integral del Riesgo en Entidades Públicas. V.7

5 Para qué se realiza el control, o que se debe: Verificar, validar, conciliar, comparar, revisar, cotejar, detectar, etc. Permite evaluar si la fuente u origen de la información que sirve para ejecutar el control es confiable para la mitigación del riesgo

 Agencia de Renovación del Territorio	INFORME	Código: FM-SEM-08
	SEGUIMIENTO EVALUACIÓN Y MEJORA	Versión: 05
	Grupo Interno de Trabajo de Control Interno	Publicado. 28-06-2024

⁶ Ejecución de la Actividad de Control	Se describe y ejecuta claramente Incompleta (Se describe o ejecuta de manera incompleta de acuerdo con lo observado y presentado en la revisión y/o las evidencias no corresponden a la ejecución del complemento o no son contundentes). No es clara la descripción del complemento o no se ejecuta.	15 10 0	15
Análisis de Desviaciones ⁷	Se describen y resuelven Ejecutadas sin evidencia Ejecutadas sin describir en control No determinadas o ejecutadas	15 10 10 0	15
⁸ Evidencia de Ejecución del Control	Completa (evidencia de Propósito, Complemento y desviaciones) Incompleta No Existe	15 10 0	15
Coherencia con el Riesgo	SI NO	5 0	5
Asociado a los controles del anexo técnico de la ISO 27001-2022	SI NO	5 0	5
Materialización del Riesgo	NO SI	5 0	5

Fuente: Elaboración propia - Grupo interno de trabajo de Control Interno – GITCI, con base en la Guía para la gestión integral del Riesgo en Entidades Públicas del DAFP.

De acuerdo con los resultados de la revisión en mesas de trabajo y las evidencias presentadas por los delegados, sobre los criterios determinados por el Auditor del GITCI se realizó la valoración y evaluación cuantitativa y cualitativa en el papel de trabajo con el fin de establecer si los controles cumplen los lineamientos en cuanto al diseño y ejecución, de esta manera el determinar si los controles existentes son efectivos para evitar la materialización de riesgos.

De acuerdo con los resultados cuantitativos para cada criterio evaluado, se generó una calificación o resultado cualitativo de la evaluación del diseño y ejecución de los controles así:

Tabla N°2:

Escala de valoración- Nivel de madurez de los controles en cuanto a diseño y ejecución			
OPTIMO	5	95- 100	Los controles permitieron prevenir la materialización del riesgo, están definidos de manera adecuada de conformidad con lo estipulado en la Guía del DAFP y MIPG en cuanto al diseño y ejecución, son coherentes con el objetivo del proceso, se soportan en procedimientos y/o políticas actualizadas y se tiene evidencia de su ejecución y registro de desviaciones.
SATISFACTORIO	4	90-94	En este nivel el control: Aunque el control permite prevenir la materialización del riesgo, presenta observaciones para la mejora; o, Se encuentra bien diseñado y se ejecuta de manera conforme sin embargo presenta debilidades en su redacción o evidencias.
ADECUADO	3	80-89	En este nivel el control: Presenta debilidades y amerita más de una mejora en su diseño, ejecución o evidencias que se pueden corregir para prevenir la materialización del riesgo.

⁶ Permite establecer cómo se ejecuta el control (fuentes de información que sean confiables), así mismo qué acciones se toman en caso de desviaciones o situaciones que se detecten. Puede darse a través de la comparación con información interna, externa o mixta. (como lo hace el responsable). Guía para la Gestión Integral del Riesgo en Entidades Públicas. V.7

⁷ Debe indicar qué pasa con las observaciones o desviaciones resultantes de ejecutar el control. Si el responsable de ejecutar el control no realiza ninguna actividad de seguimiento a las observaciones o desviaciones, o la actividad continúa a pesar de indicar esas observaciones o desviaciones, el control tendría problemas de diseño.

⁸ Permite contar con una trazabilidad en la ejecución del control. Puede ser registro físico manual o registro electrónico.

REGULAR	2	50-79	En este nivel el control: Presenta debilidades importantes por lo que se requiere replantear. Debilidades en cuanto a: diseño y ejecución (no documentado adecuadamente o sin evidencias conforme a su ejecución). En algunos casos, no previene la materialización de riesgo, o que, estando adecuadamente definido, no se ejecuta por parte del(os) responsable(s) directo(s).
DEFICIENTE	1	0-45	No cumple con los criterios para que sea un control efectivo en su diseño y ejecución.

Fuente: Elaboración propia equipo Grupo interno de trabajo de Control Interno – GITCI.

7. DESARROLLO

7.1 Objetivo 1: Verificar el diseño y ejecución de los controles a partir de los criterios definidos en la metodología y a partir de ello determinar si son adecuados para evitar la materialización de riesgos.

Una vez revisada la información aportada, dentro de la primera sesión de revisión con los delegados, se observó que, en la matriz se relacionaban numéricamente 33 riesgos en la columna A “*riesgos #*” sin embargo no correspondía al número real de riesgos, sino que correspondía al número de los activos de información. Se identificaron 87 riesgos (descritos en la columna J) frente a 33 activos de información; La columna A no corresponde al # riesgo sino al número de activo. Cada activo cuenta con 3 riesgos asociados (uno por tipología: Confidencialidad, Integridad y Disponibilidad de la información), para un total de 99 riesgos (teniendo en cuenta que algunos se repiten de acuerdo al activo de información). Por lo anterior, se sugiere ajustar el nombre de la columna para evitar una interpretación equivocada dado que no son 33 riesgos como se refieren en el archivo diligenciado.

Adicionalmente, respecto al uso del formato *FM-TI-36 V2 Formato Instrumento Mapa de Riesgos, Controles y Plan de Acción SI*, el encabezado de la matriz diligenciada con los riesgos de Seguridad Digital de la vigencia 2026 es diferente al establecido y aprobado en SIGART (en cuanto al logo, campos de identificación de versión y código del formato, así como adición de columnas no establecidas en el formato aprobado):

FM-TI-36 V2 Formato Instrumento Mapa de Riesgos, Controles y Plan de Acción SI:

1				MATRIZ RIESGOS DE SEGURIDAD DE LA INFORMACIÓN											
2				AGENCIA DE RENOVACION DEL TERRITORIO											
3															
4															
5															
6															
7															
8															
9															
10															
11															
12															
13															
14															
15															
16															
17															
18															
19															
20															
21															
22															
23															
24															
25															
26															
27															
28															
29															
30															
31															
32															
33															
34															
35															
36															
37															
38															
39															
40															
41															
42															
43															
44															
45															
46															
47															
48															
49															
50															
51															
52															
53															
54															
55															
56															
57															
58															
59															
60															
61															
62															
63															
64															
65															
66															
67															
68															
69															
70															
71															
72															
73															
74															
75															
76															
77															
78															
79															
80															
81															
82															
83															
84															
85															
86															
87															
88															
89															
90															
91															
92															
93															
94															
95															
96															
97															
98															
99															
100															

										Fecha de elaboración 05-01-2026	Fecha de actualización 05-01-2026	Fecha de Aprobación dd/mm/aaaa			Código: FM-TI-36					
														Versión 02						
														Publicación: 18/02/2026						
ión	Atributos												Plan de acción o de manejo del riesgo							
Impacto	Tipo	%	Implementación	%	Calificación del Control	Documentación	Frecuencia	Evidencia	% Probabilidad residual	Probabilidad residual	% Impacto residual	Impacto residual	Zona de riesgo final	Tratamiento	Plan de Acción	Responsable	Fecha de Implementación	Fecha Final	Evidencia	Estado
▼	▼	▼	▼	▼	▼	▼	▼	▼	▼	▼	▼	▼	▼	▼	▼	▼	▼	▼	▼	▼

Fuente: SIGART - FM-TI-36 V2 Formato Instrumento Mapa de Riesgos, Controles y Plan de Acción SI

Matriz diligenciada en formato FM-TI-36 V2 por la OTI:

COLOMBIA POTENCIA DE LA VIDA																MATRIZ RIESGOS DE SEGURIDAD DE LA INFORMACIÓN																		
AGENCIA DE RENOVACIÓN DEL TERRITORIO																																		
Riesgo #	Item	Proceso	Dependencia	Activo de Información	Tipo de activo	Amenaza (Causa Inmediata)	Vulnerabilidades (Causa raíz)	Tipo de riesgo	Descripción del Riesgo	Clasificación riesgo	Frecuencia	¿Contiene datos personales?	¿Contiene Datos personales de niños, niñas y adolescentes?	Tipo de Datos Personales	Finalidad de la Recolección de los Datos Personales	Existe la Autorización para el Tratamiento de los Datos																		
1		TODOOS	TODOOS	Información repositorio Digital (MERCURIO)	Información	Acceso no autorizado a la información del repositorio	Permisos de acceso amplios o falta de revisión periódica de usuarios habilitados	Confidencialidad	Posibilidad de que personas no autorizadas accedan a información almacenada en el repositorio digital institucional, debido a la ausencia de revisión periódica de permisos de acceso, generando exposición de información administrativa y misional.	Ejecución y administración de procesos	La actividad que conlleva el riesgo se ejecuta de 500 veces al año y máximo 5000 veces por año.	NO	NO	Dato privado	Gestión y administración de información institucional	SI																		
Fecha de elaboración 05-01-2026																	Fecha de actualización 05-01-2026			Fecha de Aprobación dd/mm/aaaa														
N		Atributos		Plan de acción o de manejo del riesgo		Fecha de implementación		Fecha Final		Evidencia		Estado		Seguimiento																				
N		Implementación	Calificación del Control	Documentación	Frecuencia	Evidencia	% Probabilidad residual	Probabilidad residual	% Impacto residual	Impacto residual	Zona de riesgo final	Tratamiento		Plan de Acción				Responsable	Fecha de implementación	Fecha Final	Evidencia	Estado	Seguimiento											
25%		Automático	25%	50%	Documentado	Continua	Con registro	30%	Baja	40%	Menor	Mediano	Reducir	Verificar trimestralmente los usuarios habilitados en el repositorio frente a los roles vigentes, gestionar por los canales definidos los ajustes de acceso requeridos, registrar las novedades identificadas, realizar seguimiento frente a su cierre y conservar registros de la gestión realizada.				El responsable de la mesa de servicios (OTI)				Trimestral	31/12/2026	Formatos de control de acceso para acceso y/o modificaciones. Paz y salvo	En curso	Seguimiento Trimestre I: 4/3/2026: Se pidió a seguridad revisar con el área de mesa de servicio, lo que se indica es que entregarán la URL donde reposa los formatos de control de acceso. Se lleva a cabo sesión EL 8/4/2026 para revisión y solicitud de evidencias, se envía correo de con actualización de matriz y acta de reunión. Se recibe URL donde la mesa de servicios aloja los formatos de control de acceso y las capturas de pantalla con las evidencias. En cuanto a los paz y salvos, no se tiene aún de parte de la OTI la recolección de estos documentos. Seguimiento Trimestre II: Se lleva a cabo sesión EL 23/06/2026 para revisión y solicitud de evidencias. Se recibe URL donde la mesa de servicios aloja los formatos de control de acceso diligenciados, la matriz de inventario de la formación y las capturas de pantalla con las evidencias. En cuanto a los paz y salvos, se recibe la ubicación donde reposan los formatos de paz y salvo diligenciados. Seguimiento Trimestre III: Realización Trimestre III								
Seguimiento																																		
Evidencias recibidas																																		
Historial de observaciones para Seguridad																																		
% avance																																		
Seguimiento Trimestre I: 4/3/2026: Se pidió a seguridad revisar con el área de mesa de servicio, lo que se indica es que entregarán la URL donde reposa los formatos de control de acceso. Se lleva a cabo sesión EL 8/4/2026 para revisión y solicitud de evidencias, se envía correo de con actualización de matriz y acta de reunión. Se recibe URL donde la mesa de servicios aloja los formatos de control de acceso y las capturas de pantalla con las evidencias. En cuanto a los paz y salvos, no se tiene aún de parte de la OTI la recolección de estos documentos. Seguimiento Trimestre II: Se lleva a cabo sesión EL 23/06/2026 para revisión y solicitud de evidencias. Se recibe URL donde la mesa de servicios aloja los formatos de control de acceso diligenciados, la matriz de inventario de la formación y las capturas de pantalla con las evidencias. En cuanto a los paz y salvos, se recibe la ubicación donde reposan los formatos de paz y salvo diligenciados. Seguimiento Trimestre III: Realización Trimestre III																	Evidencias trimestre I: Excel con inventario de formatos de acceso diligenciados de enero, febrero y marzo. https://365act.sharepoint.com/:f/f/sites/SeguridaddeLaInformacion/Documentos%20compartidos/INSTRUMENTOS%20DE%20CONTROL/Control%20de%20acceso%2067csf-1&web-1&e-1z2NKS Repositorio de formatos de paz y salvo diligenciados: Servidor Thor IP: 172.20.174.134 C:\Program Files\Apache Software Foundation\Tomcat8.5\webapps\erpSynerxis\Pagos\Archivos y captura de pantalla de los formatos en repositorio.									4/3/2026: Se pidió a seguridad revisar con el área de mesa de servicio, lo que se indica es que entregarán la URL donde reposa los formatos de control de acceso.								
Evidencias trimestre II: Excel con inventario de formatos de acceso diligenciados de abril, mayo, junio																																		

Fuente: ONEDRIVE OTI carpeta [Seguridad de la Informacion - Seguimiento 2026 Riesgos SI - Todos los documentos](#)

Fuente: ONEDRIVE OTI carpeta [Seguridad de la Informacion - Seguimiento 2026 Riesgos SI - Todos los documentos](#)

Se sugiere por tanto: corregir el archivo remitido la columna A (Riesgos#) así como la inclusión de las columnas de registro de seguimiento y porcentaje de avances al final y, solicitar a la Oficina de Planeación el ajuste del formato en SIGART. Del mismo modo se sugirió a los delegados, ajustar los nombres de las carpetas de evidencias de ejecución de las actividades del plan de manejo por cada riesgo y las principales que corresponden a la numeración de los activos de información (33) dado que se nombraron como riesgos:

SI

Seguridad de la Informacion

> Seguimiento 2026 Riesgos SI

Compartir Copiar vínculo

Todos los documentos

Nombre

Modificado

Tamaño de

Modificado

Riesgo 29

Deysi Viviana Gom

5 elementos

4 de marzo

Riesgo 30

Deysi Viviana Gom

7 elementos

4 de marzo

Riesgo 31

Deysi Viviana Gom

7 elementos

4 de marzo

Riesgo 32

Deysi Viviana Gom

5 elementos

4 de marzo

Riesgo 33

Deysi Viviana Gom

7 elementos

4 de marzo

Matriz de Riesgos 2026.xlsx

Juan Jose Sanchez

165 KB

26 de junio

SI

Seguridad de la Informacion

> Seguimiento ... > Riesgo 33

Comp

Todos los documentos

Nombre

Modificado

Plan Acción 1

Plan Acción 2

Plan Acción 3

01 Trim I Seg Riesgos SECOP-20260408.mp4

02 TRIM II Acta Seguimiento Riesgos SECOP.pdf

02 TRIM II Seg riesgosSECOP-20260622.mp4

Acta Seguimiento Riesgos SECOP Trim I.pdf

Fuente: ONEDRIVE OTI carpeta [Seguridad de la Informacion - Seguimiento 2026 Riesgos SI - Todos los documentos](#)

Lo anterior ajustado previo a la finalización del presente seguimiento:

SI

Seguridad de la Información

> Seguimiento 2026 Riesgos SI

Todos los documentos

Nombre

Activo 01

Activo 02

Activo 03

Activo 04

Activo 05

Activo 06

De la herramienta de evaluación (Papel de trabajo) el cual hace parte anexa de este informe, se extrae el siguiente resultado; En las tablas 3 y 4 se presenta el detalle de evaluación de cada de los controles evaluados de acuerdo con los criterios definidos en la metodología:

Tabla N° 3. Evaluación de controles del Mapa de Riesgos de Seguridad de la Información					
Activo de Información		Numero de Riesgo	Evaluación Controles	Valoración	Criterios con Debilidades
1	Información repositorio Digital (MERCURIO)	Riesgo 1	75	REGULAR	Evidencia Incompleta Segregación
		Riesgo 2	95	OPTIMO	Análisis de desviaciones no descritas
		Riesgo 3	100	OPTIMO	
2	Información repositorio Digital (MARTE)	Riesgo 4	75	REGULAR	Análisis de desviaciones - Evidencia
		Riesgo 5	90	SATISFACTORIO	Debilidades en redacción -Análisis de desviaciones
		Riesgo 6	100	OPTIMO	
3	Información repositorio Digital (ONEDRIVE)	Riesgo 7	80	ADECUADO	Análisis de desviaciones
		Riesgo 8	90	SATISFACTORIO	Análisis de desviaciones
		Riesgo 9	100	OPTIMO	
4	Usuario - Clave Ingreso Secop	Riesgo 10	95	OPTIMO	Evidencia de Ejecución del Control
		Riesgo 11	85	ADECUADO	Ejecución Actividad de Control Análisis de desviaciones Evidencia

 Agencia de Renovación del Territorio	INFORME		Código: FM-SEM-08
	SEGUIMIENTO EVALUACIÓN Y MEJORA		Versión: 05
	Grupo Interno de Trabajo de Control Interno		Publicado. 28-06-2024

		Riesgo 12	95	OPTIMO	Evidencia
5	Aplicación Web (https://centralpdet.renovacionterritoio.gov.co/)	Riesgo 13	90	SATISFACTORIO	Análisis de desviaciones Evidencia
		Riesgo 14	95	OPTIMO	Evidencia
		Riesgo 15	95	OPTIMO	Evidencia
		Riesgo 16	95	OPTIMO	Evidencia
6	"Aplicación Web pnis.gov.co, • https://sispnis2.direccionsustitucion-pnis.gov.co/ "	Riesgo 17	95	OPTIMO	Evidencia
		Riesgo 18	100	OPTIMO	
		Riesgo 19	100	OPTIMO	
7	Documentos físicos	Riesgo 20	100	OPTIMO	
		Riesgo 21	90	SATISFACTORIO	Análisis de desviaciones Evidencia
		Riesgo 22	85	ADECUADO	Ejecución Actividad de Control Análisis de desviaciones Evidencia
8	Bases de Datos -SQL	Riesgo 23	70	REGULAR	Segregación-Ejecución Actividad de Control Análisis de desviaciones Evidencia
		Riesgo 24	95	OPTIMO	Evidencia
		Riesgo 25	90	SATISFACTORIO	Análisis de desviaciones Evidencia
9	"Aplicación Web (• www.portal.azure.com Aplicación Web – Perseo • www.portal.azure.com Aplicación Web – Zeus	Riesgo 26	95	OPTIMO	Evidencia
		Riesgo 27	95	OPTIMO	Evidencia
		Riesgo 28	100	OPTIMO	
10	https://365uact.sharepoint.com/sites/BibliotecaBarcodeProyectosART	Riesgo 29	100	OPTIMO	
		Riesgo 30	95	OPTIMO	Evidencia
		Riesgo 31	85	ADECUADO	Ejecución Actividad de Control; Análisis de desviaciones; Evidencia
11	Software - Sistema de Gestión de Oferta	Riesgo 32	85	ADECUADO	Ejecución Actividad de Control; Análisis de desviaciones; Evidencia
		Riesgo 33	85	ADECUADO	Ejecución Actividad de Control; Análisis de desviaciones; Evidencia
		Riesgo 34	100	OPTIMO	
12	Sistema de Gestión Documental ORFEO	Riesgo 35	100	OPTIMO	
		Riesgo 36	100	OPTIMO	

 Agencia de Renovación del Territorio	INFORME		Código: FM-SEM-08
	SEGUIMIENTO EVALUACIÓN Y MEJORA		Versión: 05
	Grupo Interno de Trabajo de Control Interno		Publicado. 28-06-2024

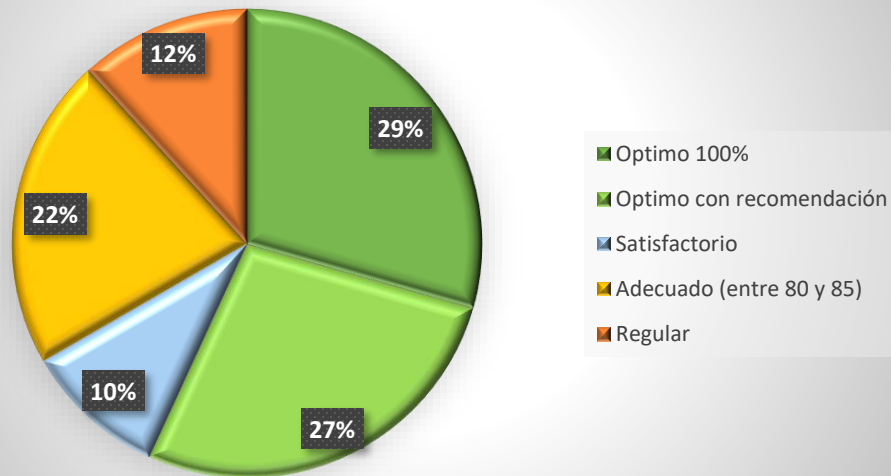
13	Cuenta de correo electrónico institucional PQRSDF	Riesgo 37	100	OPTIMO	
		Riesgo 38	95	OPTIMO	Desviaciones sin describir en control
		Riesgo 39	85	ADECUADO	Análisis de desviaciones Evidencia
14	ERP Syneris – Sistema de Información	Riesgo 40	85	ADECUADO	Análisis de desviaciones
		Riesgo 41	85	ADECUADO	Evidencia
		Riesgo 42	85	ADECUADO	Análisis de desviaciones
15	Aplicación Web - Moodle-	Riesgo 43	75	REGULAR	Ejecución Actividad de Control; Análisis de desviaciones; Evidencia
		Riesgo 44	75	REGULAR	Ejecución Actividad de Control; Análisis de desviaciones; Evidencia
		Riesgo 45	55	REGULAR	Ejecución Actividad de Control (sin ejecutar) Análisis de desviaciones Evidencia
16	Controlador de Dominio, DNS y DHCP	Riesgo 46	100	OPTIMO	
		Riesgo 47	95	OPTIMO	Evidencia
		Riesgo 48	85	ADECUADO	Ejecución Actividad de Control Análisis de desviaciones Evidencia
17	Servidores para servicio de Impresión	Riesgo 49	95	OPTIMO	Evidencia
		Riesgo 50	100	OPTIMO	
		Riesgo 51	100	OPTIMO	
		Consolidado promedio	91	SATISFACTORIO	

Fuente: Papel de trabajo evaluación riesgos SI

De los 51 riesgos y controles evaluados en cuanto a diseño y ejecución (de 17 de los 33 activos identificados en la matriz), se encontró que: 30 controles se encuentran en nivel “Optimo” respecto a su diseño y ejecución (15 calificados con 100 y 14 calificados con 95 puntos), 5 controles valorados en un nivel “Satisfactorio” con 90 puntos, 11 controles valorados en un nivel “Adecuado” (entre 80 y 85 puntos) y 6 en nivel “Regular” (uno de ellos con valoración de 55). En promedio los controles de Seguridad de la Información se encuentran en un nivel **SATISFACTORIO** con un nivel promedio del 91%, en porcentaje vislumbrados así:

 Agencia de Renovación del Territorio	INFORME	Código: FM-SEM-08
	SEGUIMIENTO EVALUACIÓN Y MEJORA	Versión: 05
	Grupo Interno de Trabajo de Control Interno	Publicado. 28-06-2024

Resumen Nivel de Evaluación Controles



Fuente: Papel de Trabajo Evaluación controles SI.

De lo anterior se concluye que: el 56% de los controles tienen un nivel “Óptimo” de diseño y ejecución de los cuales la mitad presenta recomendaciones menores para su mejora, el 10% evaluados en un nivel “Satisfactorio” con observaciones que corregidas en su redacción fortalecerían la ejecución y evidencias de los controles; el 22% de los controles evaluados en nivel “Adecuado” presentan debilidades y ameritan más de una mejora en su diseño, ejecución o evidencias; y, el 12% de los controles se encuentran en nivel “Regular” con debilidades importantes por lo que se requiere replantear en cuanto a diseño y ejecución.

Al revisar las evidencias se notó que en algunos casos se encontraron papeles de trabajo que permitieron vislumbrar la ejecución del control y las acciones tomadas en caso de desviaciones; estos papeles de trabajo tipo actas, formatos de seguimiento en Word con pantallazos e incluso grabaciones en video con la explicación de la ejecución del control; por ende, se sugiere que a partir de las revisiones del Equipo de Seguridad en calidad de 2a línea de defensa asegure que las revisiones de su parte queden claramente documentadas y no se rijan únicamente a la presentación de soportes clasificados en la columna “Evidencias” de la matriz de Riesgos, que en la mayoría de los casos donde se presentaron debilidades por este criterio evaluado, no permitieron evidenciar como tal las acciones de control (Verificación, validaciones, comparaciones, revisiones, etc) y sus resultados o conclusiones del análisis de desviaciones.

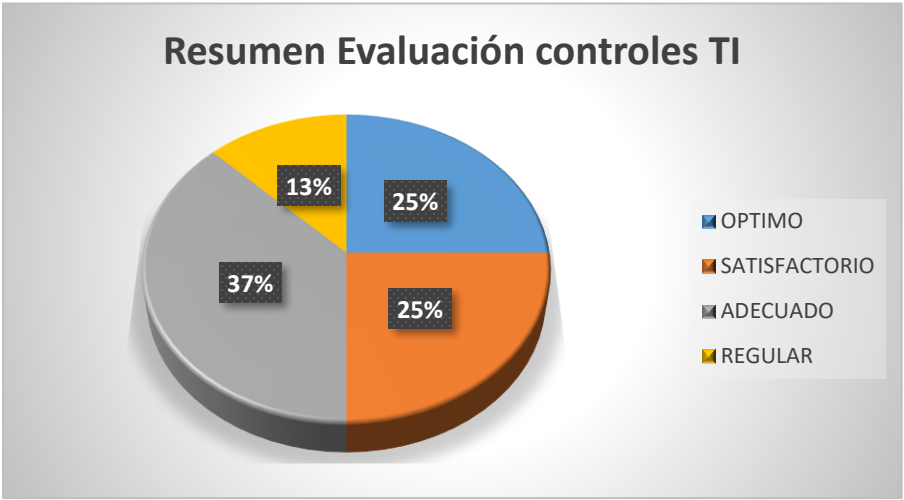
De manera general las debilidades observadas fueron en cuanto a la conservación de evidencias de ejecución de los controles, en 27 de los 51 controles evaluados esta es una característica que amerita revisarse dado que los controles pueden estar muy bien diseñados, pero si no se soportan en evidencia de acuerdo con lo descrito no es posible demostrar su debida ejecución; 22 de los controles ameritan ajustes en cuanto a la redacción considerando que no es clara la determinación y análisis de desviaciones y se encuentran mejor redactados en las acciones del plan de manejo e incluso, en 22 controles se observó que la acción del plan de manejo es casi idéntica a la actividad de control lo cual impide agregar valor al control desde el plan de manejo para mitigar el riesgo residual o ser complemento del control para robustecerlo. Lo anterior se detalla en el anexo del Informe (Papel de trabajo) el cual incluye las recomendaciones pertinentes según lo evaluado.

Respecto a la evaluación de los controles del Mapa de riesgos del proceso de Tecnología de la Información, se revisaron los 8 controles establecidos para los 4 riesgos identificados y de acuerdo con los criterios establecidos en la metodología, el resultado es el siguiente:

Tabla N° 4. Evaluación controles del Mapa de Riesgos Proceso Tecnología de la Información		
Numero de Riesgo	Evaluación Controles	Valoración
Riesgo 1	100	OPTIMO
	95	OPTIMO
Riesgo 2	80	ADECUADO
	90	SATISFACTORIO
Riesgo 3	85	ADECUADO
	80	ADECUADO
Riesgo 4	90	SATISFACTORIO
	75	REGULAR
Consolidado promedio	87	ADECUADO

Fuente: Papel de Trabajo Ev Riesgos OTI

De lo anterior se concluye que de los 8 controles establecidos para mitigar los riesgos del proceso: 2 controles se encuentran en nivel “Optimo” respecto a su diseño y ejecución, 2 controles valorados en un nivel “Satisfactorio” con 90 puntos, 3 controles valorados en un nivel “Adecuado” (entre 80 y 85 puntos) y uno (1) en nivel “Regular” (con valoración de 75). El 50% de los controles requieren revisar de fondo su diseño y ejecución. En promedio los controles del proceso de TI se encuentran en un nivel **ADECUADO** con un nivel promedio del 87%.



Fuente: Papel de Trabajo Ev Riesgos OTI

7.2 Objetivo 2: Verificar que se realice seguimiento a la ejecución de los controles y acciones del plan de manejo de riesgos y que los mismos estén soportados en evidencias.

De acuerdo con las evidencias aportadas y la evaluación cualitativa, a continuación, se describen las situaciones encontradas de los controles descritos sobre los riesgos de seguridad de la información identificados para cada activo de información de la ART y acciones del Plan de manejo:

Tabla N° 5. Resultados de Evaluación de Controles y Acciones					
N .	RIESGOS	Controles	Acciones Plan de Manejo	Evaluación	Observaciones frente al diseño y ejecución del Control y acciones del Plan de Manejo (Según Evidencias)
1	Posibilidad de que personas no autorizadas accedan a información almacenada en el repositorio digital institucional, debido a la ausencia de revisión periódica de permisos de acceso, generando exposición de información administrativa y misional.	La mesa de servicios revisa trimestralmente los permisos de acceso asignados a las carpetas de red compartidas, verificando que correspondan a los roles autorizados.	Verificar trimestralmente los usuarios habilitados en el repositorio frente a los roles vigentes, gestionar por los canales definidos los ajustes de acceso requeridos, registrar las novedades identificadas, realizar seguimiento hasta su cierre y conservar soportes de la gestión realizada.	75	Si bien en el Plan de Acción se describe y complementa claramente como se ejecuta el control, este no describe las desviaciones y, al revisar las evidencias, se soporta la ejecución de la actividad de registro de los formatos, no siendo esta la evidencia de lo definido como control con la periodicidad referida: "Revisar trimestralmente...". La acción del plan de manejo (plan de acción) es lo que debería describirse en el control; Al ser idéntica o similar a la actividad de control, no aporta valor introduce ninguna mejora frente al riesgo residual o complementar lo establecido como actividad de control. Adicionalmente, para fortalecer el control se considera que debe haber segregación de funciones debido a que quien ejecuta la actividad de registro sería el mismo que revisa si se presentan desviaciones (equipo Mesa de servicio); por lo mismo es importante segregar y asignar la verificación (control) a un responsable en particular que no sea juez y parte. En cuanto al soporte de ejecución del control se debe ajustar e incluir en las evidencias.
2	Posibilidad de modificación o eliminación no autorizada de documentos del repositorio digital institucional, debido a la falta de revisión periódica del contenido, afectando la confiabilidad de la información.	La mesa de servicios, registra las modificaciones realizadas sobre los archivos del repositorio digital mediante formatos de control de acceso.	Registrar cada solicitud de modificación de archivos del repositorio digital en los formatos de control de acceso definidos, validar la autorización del responsable del proceso antes de su ejecución, consolidar trimestralmente los registros generados y verificar su completitud.	95	El control se encuentra definido de manera más completa en la actividad del Plan de Acción considerando que registrar no sería la ejecución del control sino "validar"; No se describe/evidencia que pasa con las desviaciones y determinar la evidencia de las mismas. Se sugiere incluir la validación que hace el equipo de seguridad en la descripción del control con el fin de identificar la segregación de funciones que se aplica actualmente. La acción del plan de manejo (plan de acción) al ser idéntica o similar a la actividad de control, no aporta valor introduce ninguna mejora frente al riesgo residual o complementar lo establecido como actividad de control.

 Agencia de Renovación del Territorio	INFORME		Código: FM-SEM-08
	SEGUIMIENTO EVALUACIÓN Y MEJORA		Versión: 05
	Grupo Interno de Trabajo de Control Interno		Publicado. 28-06-2024

N	RIESGO	Controles	Acciones Plan de Manejo	Evaluación	Observaciones frente al diseño y ejecución del Control y acciones del Plan de Manejo (Según Evidencias)
3	Posibilidad de indisponibilidad de la información almacenada en el repositorio digital institucional, debido a fallas en los respaldos o a la falta de verificación periódica de su recuperabilidad, afectando la continuidad operativa de los procesos.	El administrador del repositorio digital (OTI) verifica trimestralmente la ejecución de los respaldos de la información almacenada y coordina semestralmente pruebas de restauración, documentando los resultados y gestionando las desviaciones identificadas, con el fin de asegurar la disponibilidad de la información ante eventos de pérdida.	Verificar trimestralmente los registros de ejecución de respaldos del repositorio digital, validar semestralmente pruebas de restauración, documentar los resultados obtenidos.	100	Se observa control en ejecución con las evidencias correspondientes. Se hace la observación frente a que la acción del plan de manejo (plan de acción) es similar a lo descrito en el control; Al no determinarse metodológicamente de manera complementaria, no aporta valor introduce ninguna mejora frente al riesgo residual.
4	Posibilidad de que personas no autorizadas accedan a información almacenada en el repositorio digital institucional, debido a la ausencia de revisión periódica de permisos de acceso, generando exposición de información administrativa y misional.	La mesa de servicios revisa trimestralmente los permisos de acceso asignados a las carpetas de red compartidas, verificando que correspondan a los roles autorizados.	Verificar trimestralmente los usuarios habilitados en el repositorio frente a los roles vigentes, gestionar por los canales definidos los ajustes de acceso requeridos, registrar las novedades identificadas, realizar seguimiento hasta su cierre y conservar soportes de la gestión realizada.	75	Si bien en el Plan de Acción se describe y complementa claramente como se ejecuta el control, este no describe las desviaciones y, al revisar las evidencias, se observan listados de Formatos de control de acceso para accesos y/o modificaciones gestionados por mes no siendo esta la evidencia de lo definido como control con la periodicidad referida: "Verificar trimestralmente...". Adicionalmente, para fortalecer el control se considera que debe haber segregación de funciones debido a que quien ejecuta la actividad de registro sería el mismo que revisa si se presentan desviaciones (equipo Mesa de servicios); por lo mismo es importante segregar y asignar la verificación (control) a un responsable en particular que no sea juez y parte. La acción del plan de manejo (plan de acción) al ser idéntica, similar a la actividad de control o mejor descrita, no aporta valor introduce ninguna mejora frente al riesgo residual o complementaria a la actividad de control. En cuanto al soporte de ejecución del control se debe ajustar e incluir en las evidencias.
5	Posibilidad de modificación o eliminación no autorizada de documentos del repositorio digital institucional, debido a la falta de revisión periódica del contenido, afectando la confiabilidad de la información.	La mesa de servicios registra las modificaciones realizadas sobre los archivos del repositorio digital mediante formatos de control de acceso.	Registrar cada solicitud de modificación de archivos del repositorio digital en los formatos de control de acceso definidos, validar la autorización del responsable del proceso antes de su ejecución, consolidar trimestralmente los registros generados y verificar su completitud.	90	El control se encuentra definido de manera más completa en la actividad del Plan de Acción considerando que registrar no sería la ejecución del control sino "validar"; No se describe/evidencia que pasa con las desviaciones y determinar la evidencia de las mismas. a acción del plan de manejo (plan de acción) al ser idéntica, similar a la actividad de control o mejor descrita, no aporta valor introduce ninguna mejora frente al riesgo residual o complementaria a la actividad de control. En cuanto al soporte de ejecución del control se debe ajustar e incluir en las evidencias; Respecto a estas, se presentan las mismas del control anterior, (Formatos de control de acceso para accesos diligenciados por mes) que para este caso de acuerdo con lo descrito si aplica. Se sugiere incluir la validación que hace el equipo de seguridad en la descripción del control con el fin de identificar la segregación de funciones que se aplica actualmente

 Agencia de Renovación del Territorio	INFORME		Código: FM-SEM-08
	SEGUIMIENTO EVALUACIÓN Y MEJORA		Versión: 05
	Grupo Interno de Trabajo de Control Interno		Publicado. 28-06-2024

N	RIESGO	Controles	Acciones Plan de Manejo	Evaluación	Observaciones frente al diseño y ejecución del Control y acciones del Plan de Manejo (Según Evidencias)
6	Posibilidad de indisponibilidad de la información almacenada en el repositorio digital institucional, debido a fallas en los respaldos o a la falta de verificación periódica de su recuperabilidad, afectando la continuidad operativa de los procesos.	El administrador del repositorio digital (OTI) verifica trimestralmente la ejecución de los respaldos de la información almacenada y coordina semestralmente pruebas de restauración, documentando los resultados y gestionando las desviaciones identificadas, con el fin de asegurar la disponibilidad de la información ante eventos de pérdida.	Verificar trimestralmente los registros de ejecución de respaldos del repositorio digital, validar semestralmente pruebas de restauración, documentar los resultados obtenidos.	100	Se observa control en ejecución con las evidencias correspondientes (Pruebas de restauración, Reporte de copias de respaldo, Plan de Restauración y Plan de Copias) Se hace la observación frente a que la acción del plan de manejo (plan de acción) es similar a lo descrito en el control; Al no determinarse metodológicamente de manera complementaria, no aporta valor introduce ninguna mejora frente al riesgo residual.
7	Posibilidad de que personas no autorizadas accedan a información almacenada en OneDrive institucional, debido a la falta de revisión periódica de permisos, generando exposición de información administrativa y misional.	La mesa de servicios registra mediante los formatos de control de acceso todas las solicitudes de creación, modificación y revocatoria de accesos a OneDrive institucional, conserva trazabilidad de los cambios ejecutados y consolida trimestralmente los registros generados, con el fin de controlar el acceso a la información almacenada.	Registrar cada solicitud de creación, modificación o revocatoria de accesos a OneDrive institucional, consolidar trimestralmente los formatos generados.	80	Se observan los listados y accesos a repositorio donde se encuentran los formatos de control de accesos; sin embargo, no se evidencia claramente cuales corresponden a solicitudes de one drive considerando que se enlistan todos los solicitados por mes en mesa de servicios. La actividad de control se describe como "registrar y consolidar" trimestralmente frente a lo cual se debe establecer en verbos de control y documentar la revisión y desviaciones. La acción del plan de manejo (plan de acción) al ser idéntica, similar a la actividad de control o mejor descrita, no aporta valor introduce ninguna mejora frente al riesgo residual o complementaria a la actividad de control. En cuanto al soporte de ejecución del control se debe ajustar e incluir en las evidencias.
8	Posibilidad de modificación o eliminación no autorizada de archivos almacenados en OneDrive institucional, debido a la falta de registro centralizado de cambios efectuados, afectando la confiabilidad de la información.	La mesa de servicios registra las solicitudes de modificación de archivos del repositorio digital mediante formatos de control de acceso, consolida trimestralmente los registros generados, con el fin de mantener trazabilidad sobre los cambios efectuados.	Registrar cada solicitud de modificación de archivos, validar la autorización del responsable del proceso antes de su ejecución, consolidar trimestralmente los registros.	90	El control se encuentra definido de manera más completa en la actividad del Plan de Acción considerando que registrar no sería la ejecución del control sino "validar"; No se describe/evidencia que pasa con las desviaciones y determinar la evidencia de las mismas. Se sugiere incluir la validación que hace el equipo de seguridad en la descripción del control con el fin de identificar la segregación de funciones que se aplica actualmente. Respecto a la acción del plan de manejo (plan de acción) al ser idéntica, similar a la actividad de control o mejor descrita, no aporta valor introduce ninguna mejora frente al riesgo residual o complementaria a la actividad de control.
9	Posibilidad de indisponibilidad de la información almacenada en OneDrive institucional, debido a fallas en los respaldos o ausencia de pruebas periódicas de restauración, afectando la continuidad operativa de los procesos.	La mesa de servicios verifica trimestralmente los registros de ejecución de respaldos de la información almacenada en OneDrive institucional y coordina semestralmente pruebas de restauración, documentando los resultados y consolidando los soportes generados, con el fin de asegurar la disponibilidad de la información.	Verificar trimestralmente los registros de respaldos, documentar semestralmente pruebas de restauración, consolidar los soportes obtenidos y registrar desviaciones cuando se presenten.	100	El control se encuentra definido de manera más completa en la actividad del Plan de Acción considerando que allí se describe la acción frente a la desviación. La acción del plan de manejo (plan de acción) al ser idéntica, similar a la actividad de control o mejor descrita, no aporta valor introduce ninguna mejora frente al riesgo residual o complementaria a la actividad de control. Se observa control en ejecución con las evidencias correspondientes (Pruebas de restauración, Reporte de copias de respaldo, Plan de Restauración y Plan de Copias), sin embargo, se sugiere que en la carpeta de soportes de esta actividad repose únicamente lo relacionado con el activo de información (OneDrive)

 Agencia de Renovación del Territorio	INFORME		Código: FM-SEM-08
	SEGUIMIENTO EVALUACIÓN Y MEJORA		Versión: 05
	Grupo Interno de Trabajo de Control Interno		Publicado. 28-06-2024

N	RIESGO	Controles	Acciones Plan de Manejo	Evaluación	Observaciones frente al diseño y ejecución del Control y acciones del Plan de Manejo (Según Evidencias)
10	Posibilidad de que terceros accedan al sistema SECOP utilizando credenciales institucionales, debido al manejo inadecuado o compartición de usuario y contraseña, generando exposición de información contractual y uso indebido de la plataforma.	El delegado de seguridad de la información valida trimestralmente el listado interno de funcionarios con acceso a SECOP contra la funcionarios y/o contratistas vigente, formaliza por correo institucional las solicitudes de creación, modificación o revocatoria de credenciales al administrador del servicio, y registra la socialización de la prohibición de compartición y almacenamiento visible de contraseñas, con el fin de prevenir accesos no autorizados al sistema.	Listado interno de usuarios autorizados con fecha de revisión trimestral. Correos o radicados de solicitud de alta/baja/modificación de accesos a SECOP.	95	Se sugiere especificar en la actividad de control, que se hace o cual sería la acción a seguir en caso de un acceso no autorizado al sistema. Se observan registros de listados de funcionarios con acceso a Secop y se registra ejecución del control en videos de reuniones de depuración; no se observan correos mencionados en la actividad de control ni socializaciones mencionadas (no obstante estas últimas no están determinadas como evidencia) por lo cual se sugiere que si no se presentan desviaciones se deje en un registro de la revisión, las conclusiones del mismo. Se evalúa como incompleta la evidencia debido a que solo se encuentra soporte de una revisión y la periodicidad es trimestral. Adicionalmente, se sugiere puntualizar en la acción del plan de manejo con el fin de identificar cual es la actividad dado que solo se describen soportes
11	Posibilidad de alteración de información contractual en SECOP sin detección oportuna, debido a la falta de verificación periódica de actividades realizadas con credenciales institucionales.	El delegado de seguridad de la información revisa trimestralmente los registros o reportes disponibles del sistema SECOP y los compara con los procesos contractuales internos, documentando inconsistencias y gestionando su aclaración con los responsables, con el fin de detectar modificaciones no autorizadas.	Revisar trimestralmente los reportes de operaciones disponibles en SECOP, contrastarlos con los expedientes contractuales internos, registrar hallazgos, solicitar aclaraciones cuando aplique y conservar soporte del análisis realizado.	85	Se presentan como evidencias de ejecución del control los mismos soportes del control de riesgo anterior (10), no obstante, el control se refiere a la revisión trimestral de " los registros o reportes disponibles del sistema SECOP y los compara con los procesos contractuales internos, documentando inconsistencias...". El control se encuentra bien diseñado sin embargo no se observan las evidencias correspondientes. Respecto a la acción del plan de manejo (plan de acción) al ser similar a la actividad de control, no aporta valor, o introduce mejoras frente al riesgo residual y no es complementaria a la actividad de control. En cuanto al soporte de ejecución del control se debe ajustar e incluir en las evidencias.
12	Posibilidad de indisponibilidad del acceso institucional a SECOP debido al bloqueo de credenciales por uso inadecuado, afectando la continuidad de los procesos contractuales.	El delegado de seguridad de la información gestiona trimestralmente la vigencia de accesos SECOP y mantiene canales de contacto con el proveedor del servicio para la recuperación oportuna de credenciales, asegurando la continuidad operativa del proceso.	Validar trimestralmente la vigencia de las credenciales activas, registrar incidentes de acceso, solicitar restablecimientos cuando se presenten bloqueos y documentar los tiempos de recuperación.	95	El control se encuentra definido de manera más completa en la actividad del Plan de Acción considerando que, como se describe en el control: gestionar y mantener no son verbos de control y en la acción del plan de manejo si se identifica la actividad de control "Validar trimestralmente...", por lo cual se sugiere ajustar o intercambiar las acciones. La acción del plan de manejo (plan de acción) al ser idéntica, similar a la actividad de control o mejor descrita, no aporta valor introduce ninguna mejora frente al riesgo residual o complementaria a la actividad de control. Respecto a las evidencias de ejecución, se observa una validación del semestre sin embargo en la actividad se refiere a que se hará trimestralmente por lo cual queda evaluada como incompleta la ejecución - evidencias
13	Posibilidad de que datos confidenciales sean filtrados o expuestos por vulnerabilidades técnicas	El Profesional encargado de la SGI verifica periódicamente los accesos a la Aplicación Web, asignando credenciales individuales, aplicando políticas de contraseñas seguras, revisando roles y permisos, y monitoreando intentos de acceso, asegurando que solo usuarios autorizados accedan a la información y registrando todas las actividades de control para auditoría interna.	Ejecutar revisiones periódicas de accesos y permisos por parte del Profesional encargado de la SGI, asignar credenciales individuales, aplicar políticas de contraseñas seguras, verificar roles y permisos, registrar todas las acciones de control en informes técnicos y evidencias	90	Se observan evidencias de ejecución del control de manera trimestral, sin embargo se especifica periodicidad "Bimensual" en columna AB en las evidencias se registra de esta manera. Se sugiere mejorar en la actividad de control, la descripción de lo que se hace (acción a seguir) en caso de una desviación, a quien se reporta y como aplica la segregación de funciones dentro del ejercicio del control (en caso de accesos no autorizados). Respecto a la acción del plan de manejo (plan de acción) al ser similar a la actividad de control, no aporta valor, o introduce mejoras frente al riesgo residual y no es complementaria a la actividad de control.

 Agencia de Renovación del Territorio	INFORME		Código: FM-SEM-08
	SEGUIMIENTO EVALUACIÓN Y MEJORA		Versión: 05
	Grupo Interno de Trabajo de Control Interno		Publicado. 28-06-2024

N	RIESGO	Controles	Acciones Plan de Manejo	Evaluación	Observaciones frente al diseño y ejecución del Control y acciones del Plan de Manejo (Según Evidencias)
14	Posibilidad de que la información sea alterada sin autorización debido a fallos de seguridad	El Profesional encargado de la SGI verifica periódicamente el código y las dependencias de la Aplicación Web, identifica errores de validación de datos o vulnerabilidades que puedan alterar la información, coordina la aplicación de parches o refactorización del código, y registra todas las acciones de control para garantizar que los datos no sean modificados sin autorización.	Ejecutar por parte del SOC análisis periódicos de código y dependencias, identificar vulnerabilidades que afecten la integridad, coordinar parches o refactorización, registrar resultados en informes técnicos y evidencias	95	Se observan evidencias de ejecución del control: Informes SOC, anexos informes y matriz de vulnerabilidades, sin embargo, no se observa soporte de informe técnico que concluya lo encontrado en la revisión de cada periodo o mencionado en la actividad de control como se determinó en la columna de evidencias de la matriz (no obstante que el informe SOC contiene capítulo de observaciones y recomendaciones); se sugiere dejar el soporte que registrando lo anterior, con el fin de identificar las desviaciones o no respecto a las vulnerabilidades y cuál fue la acción a seguir en cada caso, y demás evidencias que soportan en completitud el seguimiento que se realiza a partir de los informes del SOC.
15	Posibilidad de que la aplicación deje de estar disponible por explotación de vulnerabilidades	El Profesional encargado de la SGI realiza revisiones periódicas sobre configuraciones y dependencias críticas de la Aplicación Web, identifica vulnerabilidades que puedan causar interrupción del servicio, coordina la aplicación de medidas correctivas y registra todas las acciones de control para asegurar la continuidad operativa de la aplicación.	Ejecutar revisiones periódicas por parte del SOC de configuraciones y dependencias críticas, identificar vulnerabilidades que afecten disponibilidad, coordinar acciones correctivas, registrar resultados en informes técnicos y evidencias	95	Se observan evidencias de ejecución del control: Informes SOC, anexos informes y matriz de vulnerabilidades, sin embargo, no se observa soporte de informe técnico que concluya lo encontrado en la revisión de cada periodo o mencionado en la actividad de control como se determinó en la columna de evidencias de la matriz (no obstante que el informe SOC contiene capítulo de observaciones y recomendaciones); se sugiere dejar el soporte que registrando lo anterior, con el fin de identificar las desviaciones o no respecto a las vulnerabilidades y cuál fue la acción a seguir en cada caso, y demás evidencias que soportan en completitud el seguimiento que se realiza a partir de los informes del SOC.
16	Posibilidad de que datos confidenciales sean filtrados o expuestos por vulnerabilidades técnicas	El Profesional encargado de la DSCI verifica periódicamente los accesos a la Aplicación Web, asignando credenciales individuales, aplicando políticas de contraseñas seguras, revisando roles y permisos, y monitoreando intentos de acceso, asegurando que solo usuarios autorizados accedan a la información y registrando todas las actividades de control para auditoría interna.	Ejecutar revisiones periódicas de accesos y permisos por parte del Profesional encargado de la DSCI , asignar credenciales individuales, aplicar políticas de contraseñas seguras, verificar roles y permisos, registrar todas las acciones de control en informes técnicos y evidencias	95	Se observa en la carpeta de evidencias de este control, listados bimensuales de usuarios con el registro del último ingreso al sistema y roles; sin embargo, respecto a las evidencias determinadas en el plan de manejo, respecto a la "evidencia de aplicación de políticas de contraseñas y asignación de roles" no se observa en el repositorio. Se sugiere documentar la evidencia mencionada de acuerdo con la descripción del control y que se observen las conclusiones de la revisión y desviaciones, así como las acciones a seguir en caso de que se presenten.

 Agencia de Renovación del Territorio	INFORME		Código: FM-SEM-08
	SEGUIMIENTO EVALUACIÓN Y MEJORA		Versión: 05
	Grupo Interno de Trabajo de Control Interno		Publicado. 28-06-2024

N	RIESGO	Controles	Acciones Plan de Manejo	Evaluación	Observaciones frente al diseño y ejecución del Control y acciones del Plan de Manejo (Según Evidencias)
17	Posibilidad de que la información sea alterada sin autorización debido a fallos de seguridad	El Profesional encargado de la DSCI verifica periódicamente el código y las dependencias de la Aplicación Web, identifica errores de validación de datos o vulnerabilidades que puedan alterar la información, coordina la aplicación de parches o refactorización del código, y registra todas las acciones de control para garantizar que los datos no sean modificados sin autorización.	Ejecutar por parte del SOC análisis periódicos de código y dependencias, identificar vulnerabilidades que afecten la integridad, coordinar parches o refactorización, registrar resultados en informes técnicos y evidencias	95	Se tienen como soportes en el repositorio: informes de verificación del SOC, matriz de vulnerabilidades y anexos informe; no se observan <i>Informes de hallazgos, registro de parches aplicados</i> de cada periodo revisado de acuerdo con lo establecido en el control. Se revisó con el responsable de la OTI el manejo y trazabilidad de la actividad de control en lo que respecta al plan de manejo y se identificaron soportes de las acciones ejecutadas sobre el informe del SOC evidenciando además de la identificación y análisis de vulnerabilidades y eventos, correos con tickets del centro de operaciones del SOC y Excel de seguimiento que registra en hoja de casos en el cual se registra el caso con el seguimiento al cierre de este. Se sugiere mantener las evidencias en el repositorio de manera completa. Se sugiere que en la actividad de control en lugar de la palabra "coordina" de acuerdo con lo observado, se determine como "informa al responsable de la OTI" con el fin de identificar mejor la segregación y acción posterior a la desviación.
18	Posibilidad de que la aplicación deje de estar disponible por explotación de vulnerabilidades	El Profesional encargado de la DSCI realiza revisiones periódicas sobre configuraciones y dependencias críticas de la Aplicación Web, identifica vulnerabilidades que puedan causar interrupción del servicio, coordina la aplicación de medidas correctivas y registra todas las acciones de control para asegurar la continuidad operativa de la aplicación.	Ejecutar revisiones periódicas por parte del SOC de configuraciones y dependencias críticas, identificar vulnerabilidades que afecten disponibilidad, coordinar acciones correctivas, registrar resultados en informes técnicos y evidencias	100	Se tienen como soportes en el repositorio: informes de verificación del SOC, matriz de vulnerabilidades y anexos informe; no se observan <i>Informes de hallazgos, registro de parches aplicados</i> de cada periodo revisado de acuerdo con lo establecido en el control. Se revisó con el responsable de la OTI el manejo y trazabilidad de la actividad de control en lo que respecta al plan de manejo y se identificaron soportes de las acciones ejecutadas sobre el informe del SOC evidenciando además de la identificación y análisis de vulnerabilidades y eventos, correos con tickets del centro de operaciones del SOC y Excel de seguimiento que registra en hoja de casos en el cual se registra el caso con el seguimiento al cierre de este. Se sugiere mantener las evidencias en el repositorio de manera completa. Se sugiere que en la actividad de control en lugar de la palabra "coordina" de acuerdo con lo observado, se determine como "informa al responsable de la OTI" con el fin de identificar mejor la segregación y acción posterior a la desviación.
19	Posibilidad de que personas no autorizadas accedan a la documentación física, comprometiendo la confidencialidad de la información.	El responsable del archivo verifica trimestralmente los accesos a la documentación física, validando que su consulta y custodia correspondan a los responsables autorizados, gestionando los ajustes necesarios cuando se identifiquen accesos no autorizados.	Verificar trimestralmente que el acceso y la custodia de la documentación física correspondan a los responsables autorizados, revisando las condiciones de control de acceso del archivo físico y registrando los resultados de las verificaciones y las gestiones realizadas ante accesos no autorizados.	100	Se sugiere que el control especifique lo mencionado en la actividad del plan de manejo respecto a registrando los resultados de las verificaciones y las gestiones realizadas ante accesos no autorizados y no como se describe "gestionando los ajustes necesarios..." con el fin de no generar distorsión en el propósito de este; ajustar dado que la "gestión" no es claro si obedece a que se alerten los accesos no autorizados y reporten. La acción del plan de manejo es lo que debería describirse en el control y no aporta valor ni modifica el riesgo residual. Al ser idéntica a la de control, e incluso mejor redactada o más completa, no introduce ninguna mejora por lo cual se sugiere ajustar ambas actividades.

 Agencia de Renovación del Territorio	INFORME		Código: FM-SEM-08
	SEGUIMIENTO EVALUACIÓN Y MEJORA		Versión: 05
	Grupo Interno de Trabajo de Control Interno		Publicado. 28-06-2024

N	RIESGO	Controles	Acciones Plan de Manejo	Evaluación	Observaciones frente al diseño y ejecución del Control y acciones del Plan de Manejo (Según Evidencias)
20	Posibilidad de que la documentación física sea alterada, deteriorada o manipulada sin autorización, afectando la integridad de la información.	El responsable del archivo verifica trimestralmente el estado y la completitud de la documentación física, validando que no existan alteraciones, pérdidas parciales o manipulaciones no autorizadas, y gestionando las acciones correspondientes ante inconsistencias detectadas.	Verificar trimestralmente la completitud y el estado de la documentación física, validando la ausencia de alteraciones, deterioros o manipulaciones no autorizadas, y registrando las inconsistencias detectadas y las gestiones efectuadas.	100	Se observan evidencias de ejecución del control. Respecto a la acción del plan de manejo (plan de acción) al ser similar a la actividad de control, no aporta valor, o introduce mejoras frente al riesgo residual y no es complementaria a la actividad de control, por lo tanto se sugiere revisar la pertinencia o ajuste en aras de no caer en duplicidad de actividades en el caso en que con la actividad de control sea suficiente para mitigar el riesgo residual
21	Posibilidad de que fenómenos derivados del cambio climático afecten físicamente los expedientes laborales, ocasionando pérdida, deterioro o exposición no autorizada de datos personales sensibles.	El responsable del archivo verifica trimestralmente la organización y disponibilidad de la documentación física, validando que se encuentre localizada, protegida y accesible conforme a su criticidad, y gestionando los ajustes necesarios para asegurar su disponibilidad oportuna.	Verificar trimestralmente la organización, localización y disponibilidad de la documentación física conforme a su criticidad, revisando las condiciones de almacenamiento del archivo físico y registrando las verificaciones realizadas y las gestiones aplicadas para asegurar su disponibilidad oportuna.	90	Se observan como evidencias de ejecución del control, formatos del FUID diligenciados por trimestre; no se evidencian <i>Actas o reportes de inspección de condiciones de almacenamiento y conservación</i> , con lo cual se soporta la ejecución del control y acción del plan de manejo específicamente lo referido a: " <i>las condiciones de almacenamiento del archivo físico y registrando las verificaciones realizadas...</i> ". La acción del plan de manejo es lo que debería describirse en el control y no aporta valor ni modifica el riesgo residual. Al ser idéntica a la de control, e incluso mejor redactada o más completa, no introduce ninguna mejora por lo cual se sugiere ajustar ambas actividades.
22	Posibilidad de que usuarios no autorizados accedan a las bases de datos en SQL debido a una gestión inadecuada de usuarios, roles y privilegios, comprometiendo la confidencialidad de la información.	El administrador de bases de datos verifica trimestralmente los usuarios, roles y privilegios de acceso a las bases de datos en SQL, validando su correspondencia con las funciones autorizadas, y gestionando los ajustes necesarios cuando se identifiquen accesos no autorizados o excesivos.	Verificar trimestralmente los usuarios, roles y privilegios asignados en las bases de datos en SQL, validando su correspondencia con las funciones autorizadas y registrando los resultados de la revisión y las gestiones realizadas ante accesos no autorizados.	85	Se observa Listado actualizado de usuarios; no se encuentran los formatos de control de accesos determinados como evidencia sin embargo, lo que se requiere es que se pueda identificar la ejecución del control específicamente como " <i>verifica trimestralmente los usuarios, roles y privilegios de acceso a las bases de datos en SQL, validando su correspondencia con las funciones autorizadas, y gestionando los ajustes necesarios cuando se identifiquen accesos no autorizados o excesivos.</i> ". Respecto a la acción del plan de manejo (plan de acción) al ser similar a la actividad de control, no aporta valor, o introduce mejoras frente al riesgo residual y no es complementaria a la actividad de control, por lo tanto se sugiere revisar la pertinencia o ajuste en aras de no caer en duplicidad de actividades en el caso en que con la actividad de control sea suficiente para mitigar el riesgo residual

 Agencia de Renovación del Territorio	INFORME		Código: FM-SEM-08
	SEGUIMIENTO EVALUACIÓN Y MEJORA		Versión: 05
	Grupo Interno de Trabajo de Control Interno		Publicado. 28-06-2024

N	RIESGO	Controles	Acciones Plan de Manejo	Evaluación	Observaciones frente al diseño y ejecución del Control y acciones del Plan de Manejo (Según Evidencias)
23	Posibilidad de que la información almacenada en las bases de datos en SQL sea alterada o eliminada sin autorización debido a debilidades en los controles de modificación y trazabilidad, afectando la integridad de los datos.	El administrador de bases de datos define y mantiene la clasificación de la información almacenada en las bases de datos en SQL, estableciendo restricciones de modificación según su criticidad, y verificando periódicamente que los privilegios de actualización y eliminación correspondan a dicha clasificación.	Definir y mantener la clasificación de la información almacenada en las bases de datos en SQL, verificar periódicamente que los privilegios de modificación y eliminación correspondan a dicha clasificación y a las funciones autorizadas, y registrar los resultados de las verificaciones y las gestiones realizadas ante inconsistencias identificadas.	70	Si bien la actividad de control define el propósito y acción, no describe análisis de desviaciones y, con las evidencias referidas a "Listado de tablas, esquemas o conjuntos de datos con nivel de criticidad definido", de las cuales solo se encuentran en el repositorio de evidencias un archivo de "esquema de tablas 2026 SEM I", no es posible identificar que se ejecuten acciones y documenten desviaciones referidas a lo mencionado en la actividad de control y acción de plan de manejo: "verificar periódicamente que los privilegios de modificación y eliminación correspondan a dicha clasificación y a las funciones autorizadas, y registrar los resultados de las verificaciones y las gestiones realizadas ante inconsistencias identificadas"; lo anterior porque no existe evidencia que soporte su ejecución y como se hace. Adicionalmente se encuentra mejor descrita la acción del plan de manejo que el control en si mismo, siendo muy similares, lo que debe ser revisado y ajustado con el fin de contar con un control fuerte en su diseño y ejecución, soportado en evidencias.
24	Posibilidad de que las bases de datos en SQL no estén disponibles oportunamente debido a fallas técnicas o ausencia de mecanismos adecuados de respaldo y recuperación, afectando la continuidad de la operación.	El administrador de bases de datos verifica trimestralmente la ejecución y disponibilidad de los respaldos de las bases de datos en SQL, validando su capacidad de recuperación y acceso oportuno, y gestionando los ajustes necesarios ante fallas identificadas.	Verificar trimestralmente la ejecución, disponibilidad y consistencia de los respaldos de las bases de datos en SQL, validar la capacidad de recuperación de la información y registrar los resultados de las verificaciones y las gestiones realizadas ante fallas identificadas.	95	Se observa que se encuentra mejor descrita la acción del plan de manejo que el control en si mismo, siendo muy similares, lo que debe ser revisado y ajustado con el fin de contar con un control fuerte en su diseño y ejecución. En cuanto a la ejecución, se encuentra informe del primer trimestre "ANÁLISIS DE REGISTROS DE TRANSACCIÓN Y CONFIGURACIÓN DE BASE DE DATOS" en el cual se describe lo ejecutado acerca del control; no se observa informe correspondiente al 2o semestre de 2026.
25	Posibilidad de que datos confidenciales sean filtrados o expuestos por vulnerabilidades técnicas	El Profesional encargado de la SGI verifica periódicamente los accesos a la Aplicación Web, asignando credenciales individuales, aplicando políticas de contraseñas seguras, revisando roles y permisos, y monitoreando intentos de acceso, asegurando que solo usuarios autorizados accedan a la información y registrando todas las actividades de control para auditoría interna.	Ejecutar revisiones periódicas de accesos y permisos por parte del Profesional encargado de la SGI, asignar credenciales individuales, aplicar políticas de contraseñas seguras, verificar roles y permisos, registrar todas las acciones de control en informes técnicos y evidencias	90	Se observan como evidencias de ejecución del control, archivos de usuarios del portal con ultimo registro de acceso. No se encuentra la relacionada como "evidencia de aplicación de políticas de contraseñas y asignación de roles", y/o evidencia que permita identificar lo descrito como "registrar todas las acciones de control en informes técnicos y evidencias". Adicionalmente se encuentra mejor descrita la acción del plan de manejo que el control en si mismo, siendo muy similares, lo que debe ser revisado y ajustado con el fin de contar con un control fuerte en su diseño y ejecución, soportado en evidencias.

 Agencia de Renovación del Territorio	INFORME		Código: FM-SEM-08
	SEGUIMIENTO EVALUACIÓN Y MEJORA		Versión: 05
	Grupo Interno de Trabajo de Control Interno		Publicado. 28-06-2024

N	RIESGO	Controles	Acciones Plan de Manejo	Evaluación	Observaciones frente al diseño y ejecución del Control y acciones del Plan de Manejo (Según Evidencias)
26	Posibilidad de que la información sea alterada sin autorización debido a fallos de seguridad	El Profesional encargado de la SGI verifica periódicamente el código y las dependencias de la Aplicación Web, identifica errores de validación de datos o vulnerabilidades que puedan alterar la información, coordina la aplicación de parches o refactorización del código, y registra todas las acciones de control para garantizar que los datos no sean modificados sin autorización.	Ejecutar por parte del SOC análisis periódicos de código y dependencias, identificar vulnerabilidades que afecten la integridad, coordinar parches o refactorización, registrar resultados en informes técnicos y evidencias	95	Se tienen como soportes en el repositorio: informes de verificación del SOC, matriz de vulnerabilidades y anexos informe; no se observa <i>Informes de hallazgos, registro de parches aplicados</i> de acuerdo con lo establecido en las evidencias del control. Se revisó con el responsable de la OTI el manejo y trazabilidad de la actividad de control en lo que respecta al plan de manejo y se identificaron soportes de las acciones ejecutadas sobre el informe del SOC evidenciando además de la identificación y análisis de vulnerabilidades y eventos, correos con tickets del centro de operaciones del SOC y Excel de seguimiento que registra en hoja de casos en el cual se registra el caso con el seguimiento al cierre del mismo. Se sugiere mantener las evidencias en el repositorio de manera completa. Se sugiere que en la actividad de control en lugar de la palabra "coordina" de acuerdo a lo observado, se determine como "informa al responsable de la OTI" con el fin de identificar mejor la segregación y acción posterior a la desviación.
27	Posibilidad de que la aplicación deje de estar disponible por explotación de vulnerabilidades	El Profesional encargado de la SGI realiza revisiones periódicas sobre configuraciones y dependencias críticas de la Aplicación Web, identifica vulnerabilidades que puedan causar interrupción del servicio, coordina la aplicación de medidas correctivas y registra todas las acciones de control para asegurar la continuidad operativa de la aplicación.	Ejecutar revisiones periódicas por parte del SOC de configuraciones y dependencias críticas, identificar vulnerabilidades que afecten disponibilidad, coordinar acciones correctivas, registrar resultados en informes técnicos y evidencias	95	Se tienen como soportes en el repositorio: informes de verificación del SOC, matriz de vulnerabilidades y anexos informe; no se observan <i>Informes de hallazgos, registro de parches aplicados</i> de cada periodo revisado de acuerdo con lo establecido en el control. Se revisó con el responsable de la OTI el manejo y trazabilidad de la actividad de control en lo que respecta al plan de manejo y se identificaron soportes de las acciones ejecutadas sobre el informe del SOC evidenciando además de la identificación y análisis de vulnerabilidades y eventos, correos con tickets del centro de operaciones del SOC y Excel de seguimiento que registra en hoja de casos en el cual se registra el caso con el seguimiento al cierre del mismo. Se sugiere mantener las evidencias en el repositorio de manera completa. Se sugiere que en la actividad de control en lugar de la palabra "coordina" de acuerdo a lo observado, se determine como "informa al responsable de la OTI" con el fin de identificar mejor la segregación y acción posterior a la desviación.
28	Posibilidad de que usuarios no autorizados accedan a la información geográfica gestionada en la plataforma ArcGIS debido a debilidades en la gestión interna de usuarios y permisos del servicio licenciado, comprometiendo la confidencialidad de la información.	El responsable del servicio verifica trimestralmente los usuarios y perfiles de acceso asignados a la plataforma ArcGIS, validando su correspondencia con las funciones autorizadas y el licenciamiento vigente, y gestionando los ajustes necesarios con el proveedor cuando se identifiquen accesos no autorizados o indebidos.	Verificar trimestralmente los usuarios y perfiles de acceso asignados a la plataforma ArcGIS, validar su correspondencia con las funciones autorizadas y el licenciamiento vigente, y registrar los resultados de la revisión y las gestiones realizadas ante accesos no autorizados.	100	Se observan soportes de ejecución de la actividad de control. En cuanto a la actividad de control específicamente registro y análisis de desviaciones, se describe como "gestionando los ajustes necesarios" y en la acción del plan de manejo se determina "registrar los resultados de la revisión...". encontrando que las dos actividades descritas son similares y la acción del plan de manejo no complementa el control o se enfoca en tratar el riesgo residual y que se reporta un caso sin embargo no se registra claramente si corresponde a accesos no autorizados de acuerdo con los criterios del riesgo (confidencialidad) considerando que es el mismo soporte de caso reportado en el control 1, 2 y 3 del activo de información. Se sugiere documentar de manera clara las desviaciones encontradas, así como ejecución del control.

 Agencia de Renovación del Territorio	INFORME		Código: FM-SEM-08
	SEGUIMIENTO EVALUACIÓN Y MEJORA		Versión: 05
	Grupo Interno de Trabajo de Control Interno		Publicado. 28-06-2024

N	RIESGO	Controles	Acciones Plan de Manejo	Evaluación	Observaciones frente al diseño y ejecución del Control y acciones del Plan de Manejo (Según Evidencias)
29	Posibilidad de que la información geográfica gestionada en la plataforma ArcGIS sea modificada, eliminada o alterada sin autorización debido a debilidades en la gestión interna de perfiles de edición y control de cambios del servicio licenciado, afectando la integridad de la información.	El responsable del servicio verifica trimestralmente los perfiles con permisos de edición y publicación en la plataforma ArcGIS, validando su correspondencia con las funciones autorizadas y los lineamientos internos, y gestionando con el proveedor los ajustes necesarios cuando se identifiquen cambios no autorizados o inconsistencias en la información.	Verificar trimestralmente los perfiles con permisos de edición y publicación en la plataforma ArcGIS, validar su correspondencia con las funciones autorizadas y los lineamientos internos de gestión de la información, y registrar los resultados de las verificaciones y las gestiones realizadas con el proveedor ante inconsistencias identificadas.	100	Se observan soportes de ejecución de la actividad de control. La actividad de control y la acción del plan de manejo son similares; En cuanto a la actividad de control específicamente registro y análisis de desviaciones, se describe como "gestionando con el proveedor los ajustes necesarios"; en la acción del plan de manejo se determina "registrar los resultados de las verificaciones...". en las evidencias del repositorio se observa un caso reportado sin embargo no se registra claramente si corresponde a incumplimiento de lineamientos internos o cambios no autorizados de acuerdo con los criterios del riesgo (integridad) considerando que es el mismo soporte de caso reportado en el control 1, 2 y 3 del activo de información. Se sugiere documentar de manera clara las desviaciones encontradas, así como ejecución del control. Se sugiere que la acción del plan de manejo complemente el control enfocándose a en tratar el riesgo residual.
30	Posibilidad de que la plataforma ArcGIS no esté disponible oportunamente debido a fallas del proveedor o interrupciones del servicio, sumado a debilidades en la gestión interna de la continuidad del servicio licenciado, afectando la operación institucional.	El responsable del servicio verifica trimestralmente la disponibilidad de la plataforma ArcGIS conforme a los niveles de servicio acordados, gestionando con el proveedor las incidencias de indisponibilidad y validando la ejecución de las acciones definidas para asegurar la continuidad del servicio.	Verificar trimestralmente la disponibilidad de la plataforma ArcGIS conforme a los niveles de servicio acordados, realizar seguimiento a las incidencias de indisponibilidad gestionadas con el proveedor y registrar los resultados de las verificaciones y las gestiones realizadas para asegurar la continuidad del servicio.	95	Se observan soportes de gestión de incidente de acuerdo a lo descrito en la actividad de control. La actividad de control y la acción del plan de manejo son similares; Se sugiere que la acción del plan de manejo complemente el control enfocándose a en tratar el riesgo residual. En cuanto a la actividad de control específicamente registro y análisis de desviaciones, se describe como "gestionando con el proveedor las incidencias de indisponibilidad"; en la acción del plan de manejo se determina "registrar los resultados de las verificaciones..."; en las evidencias del repositorio se observa un caso reportado sin embargo no se registra claramente si corresponde a incumplimiento de lineamientos internos o cambios no autorizados de acuerdo a los criterios del riesgo (integridad). Se sugiere documentar de manera clara las desviaciones encontradas así como ejecución del control dado que dentro de las evidencias relacionadas para la ejecución de este control se describen las siguientes no aportadas en el repositorio: <i>Registros de seguimiento a incidentes de indisponibilidad. Comunicaciones o tickets gestionados con el proveedor frente a fallas del servicio.</i>
31	Posibilidad de que la información del Sistema de Gestión de Oferta sea divulgada a personas no autorizadas debido a debilidades en los mecanismos de autenticación y control de accesos, afectando la confidencialidad de la información y la confianza en los procesos asociados.	El administrador del servicio verifica que todos los usuarios del Sistema de Gestión de Oferta tengan credenciales individuales, roles asignados conforme al principio de mínimo privilegio y mecanismos de autenticación activa, revisando los registros de acceso y reportes cada trimestre, con el fin de prevenir la divulgación no autorizada de la información y proteger la confidencialidad del sistema.	Configurar mecanismos de autenticación segura acordes a la criticidad del Sistema de Gestión de Oferta, restringir el acceso a la información según perfiles autorizados, monitorear y registrar los eventos de acceso para identificar comportamientos anómalos, validar periódicamente la vigencia de los usuarios habilitados y corregir oportunamente las desviaciones que puedan afectar la confidencialidad de la información.	85	Se encuentra en las evidencias listados de usuarios interno y externos así como de las URL en donde se ubican los formatos de control de acceso, no observando consistencia de las evidencias con la ejecución del control y que de manera clara o específica se documente como se verifico, que se encontró y si se presentaron desviaciones o no. Si bien en la acción del plan de manejo se puede observar descrita la ejecución del control en cuanto al análisis de desviaciones, esto debería describirse en el control. Se sugiere ajustar la redacción del control y registro de ejecución dejando una evidencia tangible con el fin de documentar los resultados de la revisión de manera clara

 Agencia de Renovación del Territorio	INFORME		Código: FM-SEM-08
	SEGUIMIENTO EVALUACIÓN Y MEJORA		Versión: 05
	Grupo Interno de Trabajo de Control Interno		Publicado. 28-06-2024

N	RIESGO	Controles	Acciones Plan de Manejo	Evaluación	Observaciones frente al diseño y ejecución del Control y acciones del Plan de Manejo (Según Evidencias)
32	Posibilidad de que la información del Sistema de Gestión de Oferta sea modificada, alterada o eliminada de manera no autorizada debido a debilidades en los controles de autorización y trazabilidad, generando inconsistencias en la información y afectando la confiabilidad de los procesos institucionales.	El administrador del servicio protege la integridad de la información del Sistema de Gestión de Oferta mediante la asignación de privilegios y roles autorizados, el control de modificaciones de la información y el registro de todas las operaciones realizadas trimestralmente, revisando la consistencia de los datos, con el fin de prevenir alteraciones no autorizadas y asegurar la confiabilidad de la información.	Definir y aplicar roles y privilegios conforme al principio de mínimo acceso necesario, implementar controles que restrinjan la modificación de la información a usuarios autorizados, registrar y monitorear las operaciones realizadas sobre la información, validar periódicamente la coherencia e integridad de los datos y corregir oportunamente las desviaciones detectadas que puedan afectar la integridad de la información del sistema.	85	La actividad de control no define análisis de desviaciones y acciones a seguir en caso de que se presenten; en la acción del plan de manejo se puede observar descrita la ejecución del control en cuanto al análisis de desviaciones, lo cual debería describirse en el control. Se encuentran como evidencias matrices de rol por módulo de cada trimestre y URL con formatos de control de acceso, sin embargo, no es claro cómo se ejecuta y el resultado registrado. Se sugiere ajustar la redacción del control y registro de ejecución con el análisis de desviaciones dejando una evidencia tangible de ello con el fin de documentar los resultados de la validación de la integridad de los datos.
33	Posibilidad de que el Sistema de Gestión de Oferta no se encuentre disponible de manera oportuna debido a fallas técnicas o eventos no controlados, afectando la continuidad de los procesos misionales y la prestación de los servicios de la entidad.	El administrador del servicio en conjunto con el responsable de la OTI (backup) asegura la disponibilidad del Sistema de Gestión de Oferta mediante la implementación de esquemas de respaldo, mecanismos de recuperación ante fallas y monitoreo continuo de la operación, revisando periódicamente los registros de respaldo y los reportes de incidentes cada trimestre, con el fin de garantizar la continuidad de los servicios y reducir el impacto de fallas o indisponibilidades.	Implementar esquemas de respaldo del Sistema de Gestión de Oferta acordes a su criticidad, configurar mecanismos de recuperación que permitan restablecer el sistema de manera oportuna ante fallas o incidentes, validar periódicamente la efectividad de los respaldos y procesos de recuperación, corregir oportunamente las desviaciones que puedan afectar la disponibilidad del sistema y la continuidad de los servicios institucionales.	85	La actividad de control no define análisis de desviaciones y acciones a seguir en caso de que se presenten; en la acción del plan de manejo se puede observar descrita la ejecución del control en cuanto al análisis de desviaciones, lo cual debería describirse en el control. Se encuentran como evidencias: Reportes de Copias de respaldo mensuales, sin embargo, no es claro cómo se ejecuta y el resultado registrado de qué manera evidencia la ejecución del control y acción del plan de manejo de acuerdo a lo descrito. Se sugiere ajustar la redacción del control y registro de ejecución con el análisis de desviaciones dejando una evidencia tangible de ello con el fin de documentar los resultados de la validación de la integridad de los datos.
34	Posibilidad de que la información y documentos del Sistema de Gestión Documental ORFEO sean divulgados a personas no autorizadas debido a deficiencias en los mecanismos de autenticación y control de accesos, afectando la confidencialidad y la confianza en los procesos documentales.	El Profesional administrador (OTI) verifica que todos los usuarios del Sistema de Gestión Documental ORFEO tengan credenciales individuales, roles asignados conforme al principio de mínimo privilegio y mecanismos de autenticación activa, revisando los registros de acceso cada trimestre, con el fin de prevenir la divulgación no autorizada de la información y proteger la confidencialidad de los documentos.	Configurar mecanismos de autenticación segura y asignación de roles según perfiles autorizados, monitorear y registrar los eventos de acceso al sistema para detectar accesos indebidos, validar periódicamente la vigencia de los usuarios habilitados y corregir oportunamente las desviaciones que puedan afectar la confidencialidad de los documentos y la información del sistema.	100	Se observan evidencias de ejecución del control de manera trimestral (formatos de control de acceso, Reporte de usuarios activos, casos de mesa de ayuda). Se sugiere en el Excel de USUARIOS ORFEO NOVEDADES incluir al final una columna para identificar los que fueron objeto de la verificación respecto a los accesos e identificar los que presentaron desviaciones frente a los accesos y/o ajustes del aplicativo ORFEO como consecuencia de la ejecución del control.

 Agencia de Renovación del Territorio	INFORME		Código: FM-SEM-08
	SEGUIMIENTO EVALUACIÓN Y MEJORA		Versión: 05
	Grupo Interno de Trabajo de Control Interno		Publicado. 28-06-2024

N	RIESGO	Controles	Acciones Plan de Manejo	Evaluación	Observaciones frente al diseño y ejecución del Control y acciones del Plan de Manejo (Según Evidencias)
35	Posibilidad de que la información y documentos almacenados en el Sistema de Gestión Documental ORFEO sean modificados o eliminados de manera no autorizada debido a debilidades en la asignación de privilegios y trazabilidad, generando inconsistencias en los documentos y afectando la confiabilidad de los procesos.	El Profesional administrador (OTI) del servicio establece mecanismos de protección a la integridad de la información y documentos del Sistema de Gestión Documental ORFEO mediante la asignación de privilegios autorizados, el control de modificaciones de documentos y el registro de todas las operaciones realizadas, revisando la consistencia de los datos cada trimestre, con el fin de prevenir alteraciones no autorizadas y garantizar la confiabilidad de la información.	Definir y aplicar roles y privilegios conforme al principio de mínimo acceso necesario, implementar controles que restrinjan la modificación de los documentos a usuarios autorizados, registrar y monitorear las operaciones realizadas sobre la información, validar periódicamente la coherencia e integridad de los documentos y corregir oportunamente las desviaciones detectadas que puedan afectar la integridad del sistema.	100	Se observan evidencias de ejecución del control de manera trimestral (formatos de control de acceso, Reporte de usuarios activos, casos de mesa de ayuda). Se sugiere en el Excel de USUARIOS ORFEO NOVEDADES incluir al final una columna para identificar los que fueron objeto de la verificación respecto a los accesos e identificar los que presentaron desviaciones relacionadas con la confiabilidad de la información del aplicativo ORFEO
36	Posibilidad de que el Sistema de Gestión Documental ORFEO no esté disponible de manera oportuna debido a fallas técnicas o incidentes, afectando la continuidad de los procesos documentales y la prestación de servicios de la entidad.	El Profesional administrador (OTI) del servicio y la mesa de servicio (OTI) asegura la disponibilidad del Sistema de Gestión Documental ORFEO mediante la implementación de esquemas de respaldo, mecanismos de recuperación ante fallas y monitoreo continuo de la operación, revisando los registros de respaldo y reportes de incidentes cada trimestre, con el fin de garantizar la continuidad del servicio y reducir el impacto de indisponibilidades.	Implementar esquemas de respaldo del Sistema de Gestión Documental ORFEO según su criticidad, configurar mecanismos de recuperación que permitan restablecer el sistema ante fallas o incidentes, monitorear continuamente el estado operativo del sistema para detectar indisponibilidades, validar periódicamente la efectividad de los respaldos y procesos de recuperación, y corregir oportunamente las desviaciones que puedan afectar la disponibilidad del sistema y la continuidad de los procesos documentales.	100	La actividad de control no define análisis de desviaciones y acciones a seguir en caso de que se presenten; en la acción del plan de manejo se puede observar descrita la ejecución del control en cuanto al análisis de desviaciones, lo cual debería describirse en el control. Se observan evidencias de ejecución del control: Plan de Copias de Respaldo y Recuperación de Datos, formatos de EJECUCIÓN PRUEBAS DE RESTAURACIÓN DE BACKUPS, Reporte de copias de respaldo mensuales (hasta Junio de 2026)
37	Posibilidad de que la información contenida en la cuenta de correo institucional utilizada para la gestión de PQRSDf sea divulgada a personas no autorizadas debido a fallas en los mecanismos de autenticación y control de accesos, comprometiendo la confidencialidad y la confianza en la gestión de los requerimientos ciudadanos.	El profesional de la mesa de servicios(OTI) verifica que el acceso a la cuenta se limite exclusivamente a su uso autorizado, que las credenciales se mantengan seguras y que la información enviada o recibida sea manejada según protocolos de confidencialidad, revisando los registros de acceso y reportes de actividad cada trimestre , con el fin de prevenir la divulgación no autorizada de información y proteger la confidencialidad del sistema de correo.	Configurar la autenticación multifactor y asignación de roles por perfil de usuario, monitorear y registrar los accesos a las cuentas de correo institucional, revisar periódicamente los registros de actividad y credenciales, validar la vigencia de los usuarios habilitados y corregir oportunamente las desviaciones que puedan afectar la confidencialidad de la información de PQRSDf.	100	Se observan evidencias de ejecución del control: Revisión de autenticación multifactor del correo de PQRDS de la DSCI y del correo de enlace al ciudadano, con un consolidado de casos

 Agencia de Renovación del Territorio	INFORME		Código: FM-SEM-08
	SEGUIMIENTO EVALUACIÓN Y MEJORA		Versión: 05
	Grupo Interno de Trabajo de Control Interno		Publicado. 28-06-2024

N	RIESGO	Controles	Acciones Plan de Manejo	Evaluación	Observaciones frente al diseño y ejecución del Control y acciones del Plan de Manejo (Según Evidencias)
38	Posibilidad de que la información contenida en la cuenta de correo institucional para PQRSDF sea modificada, alterada o eliminada de manera no autorizada, debido a deficiencias en los controles de acceso y trazabilidad, generando inconsistencias en la gestión de requerimientos ciudadanos.	El profesional de la mesa de servicios(OTI) establece mecanismos para la integridad de la información gestionada mediante la supervisión de operaciones y la revisión periódica de los correos enviados y recibidos, revisando los reportes trimestrales , con el fin de prevenir alteraciones no autorizadas y garantizar la confiabilidad de la información.	Definir y aplicar roles y privilegios conforme al principio de mínimo acceso necesario, implementar controles que restrinjan la modificación o eliminación de correos a usuarios autorizados, registrar y monitorear las operaciones realizadas, validar periódicamente la coherencia e integridad de la información gestionada y corregir oportunamente las desviaciones detectadas que puedan afectar la integridad del sistema de correo.	95	Se observan evidencias de ejecución del control: Restricciones al buzón de correo y reporte trimestral de control. Se sugiere indicar en el control que pasa con las desviaciones refiriendo cual sería la acción a seguir o las evidencias que se generen de las mismas, es decir, si se presenta una alteración no autorizada, donde, como o a quien se reporta previo a las correcciones señaladas en la actividad del plan de acción.
39	Posibilidad de que la cuenta de correo institucional utilizada para PQRSDF no esté disponibles de manera oportuna debido a fallas técnicas o incidentes, afectando la continuidad de la gestión de requerimientos ciudadanos.	El profesional de la mesa de servicios(OTI) establece mecanismos para la disponibilidad de la cuenta mediante la configuración de respaldos, la recuperación ante fallas y el monitoreo continuo de su operación, revisando periódicamente los registros de respaldo cada trimestre , con el fin de garantizar la continuidad de la gestión de PQRSDF y reducir el impacto de indisponibilidades.	Implementar esquemas de respaldo de las cuentas de correo institucional, configurar mecanismos de recuperación que permitan restablecer la disponibilidad ante fallas o incidentes, monitorear continuamente el estado operativo del sistema, validar periódicamente la efectividad de los respaldos y procesos de recuperación, y corregir oportunamente las desviaciones que puedan afectar la disponibilidad del correo y la continuidad de la gestión de PQRSDF.	85	Una vez revisadas las evidencias del repositorio para este control, se observan reportes de backups y copias de respaldo generales, en las cuales no se observa claramente la ejecución del control sobre las cuentas de correo de PQRSDF. Es pertinente dejar documentada la evidencia de la revisión de los registros con las conclusiones de lo analizado y si se presentaron o no desviaciones.
40	Posibilidad de que la información gestionada en el ERP Syneris sea accedida por personas no autorizadas debido a deficiencias en los controles de acceso y autenticación, comprometiendo la confidencialidad de la información institucional.	El Administrador del ERP Syneris (OTI) verifica que los accesos al sistema se encuentren asignados mediante credenciales individuales, roles definidos según funciones y el principio de mínimo privilegio, revisando trimestralmente los usuarios habilitados y los registros de acceso, con el fin de prevenir accesos no autorizados y proteger la confidencialidad de la información gestionada en el ERP.	Validar periódicamente los usuarios y roles configurados en el ERP Syneris, ajustar privilegios conforme a las funciones autorizadas, monitorear los accesos al sistema, registrar y analizar eventos asociados a intentos de acceso no autorizado y corregir oportunamente las desviaciones que puedan afectar la confidencialidad de la información institucional.	85	En cuanto a la actividad de control específicamente registro y análisis de desviaciones, se describe como " con el fin de prevenir accesos no autorizados"; en la acción del plan de manejo se encuentra mejor descrita la actividad de control sin embargo es importante determinar el actuar en caso de desviaciones derivadas de los descrito en la acción del plan de manejo; esto debería hacer parte de la descripción del control. Se encuentran como evidencia archivos de Solicitudes de control de acceso, archivo con registro fotográfico y URL de repositorio de formatos de control de acceso (todos los de cada mes), archivos de usuarios activos e inactivos. Se sugiere que en el archivo de solicitudes de control de acceso que reporta los accesos por trimestre, se describa en una columna lo que fue objeto de revisión de acuerdo al control descrito y resultado del monitoreo a los accesos dado que no es claro cómo fue la revisión o que concluye respecto del activo de información

 Agencia de Renovación del Territorio	INFORME		Código: FM-SEM-08
	SEGUIMIENTO EVALUACIÓN Y MEJORA		Versión: 05
	Grupo Interno de Trabajo de Control Interno		Publicado. 28-06-2024

N	RIESGO	Controles	Acciones Plan de Manejo	Evaluación	Observaciones frente al diseño y ejecución del Control y acciones del Plan de Manejo (Según Evidencias)
41	Posibilidad de que la información registrada en el ERP Synergis sea modificada o eliminada de manera no autorizada debido a deficiencias en los controles de autorización y trazabilidad, generando inconsistencias en los procesos financieros y administrativos.	El Administrador del ERP Synergis(OTI), mediante la asignación controlada de permisos de modificación, el registro y revisión de eventos del sistema y la verificación periódica de transacciones críticas, revisando trimestralmente los reportes del ERP, con el fin de prevenir alteraciones no autorizadas y garantizar la confiabilidad de la información.	Configurar y mantener controles de autorización para operaciones del ERP, analizar eventos asociados a modificaciones no autorizadas y aplicar acciones correctivas oportunas ante desviaciones que puedan afectar la integridad de los datos.	85	No se describe claramente orientación del análisis de desviaciones y acción generada si aplica. Se encuentran como evidencia archivos de Logs de auditoría y registro de cambios, archivos de usuarios activos e inactivos; sin embargo no es concluyente o claramente observable la ejecución del control y resultados de las revisiones realizadas con las evidencias aportadas de manera que se observe análisis de eventos del periodo y aplicación de correctivos. Se sugiere revisar y ajustar redacción de la actividad de control
42	Posibilidad de que el ERP Synergis no se encuentre disponible de manera oportuna debido a fallas técnicas o incidentes, afectando la continuidad de los procesos financieros, administrativos y operativos de la entidad.	El Administrador del ERP Synergis (OTI) - Mesa de servicios (OTI) a través de diferentes mecanismos como la ejecución de respaldos periódicos, la verificación de los mecanismos de recuperación y el monitoreo continuo del estado operativo del ERP, revisando trimestralmente los registros de respaldo y los reportes de incidentes, con el fin de garantizar la continuidad del servicio y reducir el impacto de indisponibilidades.	Implementar y mantener esquemas de respaldo del ERP Synergis conforme a su criticidad, verificar periódicamente la efectividad de los procesos de recuperación, monitorear la disponibilidad y desempeño del sistema, registrar incidentes de indisponibilidad y ejecutar acciones correctivas oportunas para asegurar la continuidad de los procesos institucionales.	85	Una vez revisadas las evidencias del repositorio para este control, se observan reportes de backups y copias de respaldo generales, Plan de copias y plan de restauración; sin embargo, no se observa claramente la ejecución del control sobre la revisión trimestral de los registros de respaldo e incidentes en cuanto a que sea concluyente sobre el activo y la ejecución del control. Es pertinente dejar documentada la evidencia de la revisión de los registros con las conclusiones de lo analizado y si se presentaron o no desviaciones.
43	Posibilidad de que personas no autorizadas accedan a la información académica y evaluaciones de funcionarios, vulnerando la confidencialidad de los datos.	El administrador del sistema Moodle (OTI) valida los accesos de los usuarios mediante la revisión del listado de cuentas activas (LDAP), la confirmación de roles asignados y la desactivación de usuarios inactivos a través del panel de administración de la plataforma, con una periodicidad trimestral y por evento cuando se presenten retiros o cambios de rol, con el fin de prevenir accesos no autorizados a la información del sistema.	Actualizar trimestralmente el inventario de usuarios del sistema, ejecutar jornadas formales de revisión de roles y permisos, registrar los resultados de cada validación, gestionar oportunamente las solicitudes de creación, modificación o eliminación de cuentas, realizar seguimiento a los hallazgos detectados y documentar las acciones correctivas implementadas para fortalecer el control de accesos.	75	Se encuentra como evidencia un reporte de la plataforma MOODLE con casos de vigencias 2023, 2024 y 2025. Lo anterior no es evidencia de ejecución del control ni acción del plan de manejo de acuerdo a lo descrito ni con la periodicidad definida.

 Agencia de Renovación del Territorio	INFORME		Código: FM-SEM-08
	SEGUIMIENTO EVALUACIÓN Y MEJORA		Versión: 05
	Grupo Interno de Trabajo de Control Interno		Publicado. 28-06-2024

N	RIESGO	Controles	Acciones Plan de Manejo	Evaluación	Observaciones frente al diseño y ejecución del Control y acciones del Plan de Manejo (Según Evidencias)
44	Posibilidad de que se altere la información académica o los resultados de evaluación de los funcionarios sin autorización, afectando la confiabilidad de los procesos de capacitación y toma de decisiones.	El administrador del sistema Moodle (OTI) validar las modificaciones realizadas sobre calificaciones y contenidos mediante la revisión periódica de los registros de auditoría del sistema y la comparación de los cambios efectuados frente a las autorizaciones otorgadas, utilizando las herramientas de log y reportes de la plataforma, con una periodicidad mensual y por evento cuando se detecten inconsistencias, con el fin de asegurar la integridad de la información gestionada en el sistema.	Configurar y mantener habilitados los registros de auditoría del sistema, ejecutar revisiones mensuales de los cambios críticos, documentar los resultados de cada validación, gestionar la corrección de modificaciones no autorizadas, realizar seguimiento a los hallazgos identificados y registrar las acciones implementadas para fortalecer el control sobre la información.	75	Se encuentra como evidencia un reporte de la plataforma MOODLE con casos de vigencias 2023, 2024 y 2025. Lo anterior no es evidencia de ejecución del control ni acción del plan de manejo de acuerdo con lo descrito ni con la periodicidad definida (mensual). La evidencia no identifica la revisión de registros de auditoría del sistema comparados con los cambios frente a las autorizaciones.
45	Posibilidad de que la indisponibilidad del sistema Moodle impida el acceso a los procesos de capacitación y evaluación de funcionarios, afectando la continuidad de la operación institucional.	El responsable de la mesa de servicios verifica la ejecución de los respaldos del sistema Moodle mediante la revisión de los registros automáticos del servidor y la validación del almacenamiento correcto de los archivos y la base de datos en repositorios definidos, con una periodicidad trimestral para la validación de restauración, con el fin de asegurar la recuperación oportuna del servicio ante fallas.	Definir y ejecutar un cronograma formal de respaldos automáticos, realizar pruebas semestrales de restauración en un ambiente controlado, gestionar los ajustes necesarios cuando se identifiquen fallas, registrar los incidentes de indisponibilidad presentados y hacer seguimiento a las acciones correctivas implementadas para fortalecer la continuidad del servicio.	55	En las evidencias aportadas no se observan pruebas de restauración ni copias de respaldo del activo de información Moodle sino de otros activos. Por lo tanto, no se registra evidencia de ejecución del control
46	Posibilidad de que usuarios no autorizados accedan a la información de autenticación y directorio activo, comprometiendo la confidencialidad de las credenciales y datos institucionales.	El administrador de infraestructura (OTI) verifica y valida las cuentas con privilegios administrativos del controlador de dominio mediante la revisión del listado de usuarios y grupos de seguridad, comparando los accesos otorgados frente a las autorizaciones formales registradas, utilizando las consolas de administración del directorio activo, con una periodicidad trimestral y por evento ante cambios de personal, con el fin de prevenir accesos no autorizados al sistema.	Actualizar trimestralmente el inventario de cuentas privilegiadas, ejecutar revisiones formales de accesos administrativos, gestionar la eliminación de permisos innecesarios para fortalecer el control de accesos.	100	Se observan evidencias de ejecución de la actividad de control

 Agencia de Renovación del Territorio	INFORME		Código: FM-SEM-08
	SEGUIMIENTO EVALUACIÓN Y MEJORA		Versión: 05
	Grupo Interno de Trabajo de Control Interno		Publicado. 28-06-2024

N	RIESGO	Controles	Acciones Plan de Manejo	Evaluación	Observaciones frente al diseño y ejecución del Control y acciones del Plan de Manejo (Según Evidencias)
47	Posibilidad de que se alteren configuraciones críticas del dominio, DNS o DHCP sin autorización, afectando la confiabilidad y estabilidad de la red institucional.	El administrador de infraestructura (OTI) verifica los cambios realizados en políticas de dominio, configuraciones DNS y DHCP mediante la revisión de registros del sistema y la comparación contra solicitudes de cambio aprobadas, utilizando las consolas administrativas y bitácoras de eventos, con una periodicidad semestral y por evento ante cambios críticos, con el fin de asegurar la integridad de las configuraciones.	Implementar un registro formal de solicitudes de cambio, ejecutar revisiones trimestrales de configuraciones críticas, documentar los resultados, gestionar la reversión de cambios no autorizados para fortalecer el control de cambios.	95	Se observa como evidencia un informe de eventos del sistema y del administrador (FORTINET) del primer trimestre de 2026; La evidencia se considera incompleta considerando que no es contundente para identificar el resultado de la comparación contra las solicitudes de cambio aprobadas, ni se observa el "registro formal de solicitudes de cambio" trimestral de acuerdo a lo establecido en la acción del plan de manejo. Se tiene el video de seguimiento de Seguridad de la Información -SI-, en el cual se da la explicación de la ejecución del control y las evidencias en el sistema; en la misma se propuso que SI realice el seguimiento sobre el control y mejoras. Se sugiere dejar en el repositorio las evidencias mencionadas en el seguimiento con la delegada de SI y quedo como compromiso sin embargo no se encuentran a la fecha de revisión del GIT de Control Interno.
48	Posibilidad de que la indisponibilidad del controlador de dominio, DNS o DHCP impida la autenticación y conectividad de los usuarios, afectando la operación institucional.	El administrador de infraestructura (OTI) verifica la ejecución de respaldos del controlador de dominio y servicios asociados mediante la revisión de logs automáticos y la validación del almacenamiento correcto de la información en repositorios definidos, realizando pruebas de restauración controladas, con una periodicidad semestral, con el fin de asegurar la recuperación oportuna del servicio.	Definir y ejecutar un cronograma formal de respaldos, realizar pruebas semestrales de restauración en ambiente controlado, gestionar ajustes ante fallas detectadas, registrar incidentes de indisponibilidad.	85	Se encuentran en el repositorio evidencias de copias de respaldo y back ups de ORFEO, Servidor de Base de Datos Servidor de Archivo, Servidor de Correo, Servidor Nube, Servidor de Aplicación, MARTE. No se observa un registro que permita comprobar la ejecución del control evidenciando la comparación establecida en el control y el registro mencionado en la acción del plan de manejo.
49	Posibilidad de que información enviada a impresión sea accedida o divulgada por personal no autorizado.	El Administrador de infraestructura tecnológica verifica trimestralmente los usuarios con acceso a los servidores de impresión, cotejando permisos contra listados oficiales de personal autorizado; conserva registros de revisión y, ante accesos no autorizados, solicita su eliminación inmediata y documenta la novedad.	Revisar trimestralmente los usuarios con acceso a los servidores de impresión, retirar permisos no autorizados y registrar los ajustes realizados, siendo el responsable de la mesa de servicios (OTI).	95	Se observan los reportes de usuarios trimestrales y listado de usuarios autorizados, sin embargo no se tiene un registro o evidencia del resultado de ejecución del control "cotejar los permisos" así como las desviaciones si se presentaron o no.
50	Posibilidad de que se alteren configuraciones del servidor afectando el procesamiento correcto de documentos.	El Administrador de infraestructura tecnológica valida trimestralmente que los cambios realizados cuenten con solicitud y aprobación previa, revisando tickets y bitácoras; conserva registros y, ante cambios no autorizados, revierte la configuración y reporta el incidente.	Verificar trimestralmente los cambios ejecutados en los servidores de impresión, validar que cuenten con aprobación formal y documentar desviaciones identificadas, siendo el responsable de la mesa de servicios (OTI).	100	Se observan evidencias de ejecución del control en formato de seguimiento con pantallazos

 Agencia de Renovación del Territorio	INFORME		Código: FM-SEM-08
	SEGUIMIENTO EVALUACIÓN Y MEJORA		Versión: 05
	Grupo Interno de Trabajo de Control Interno		Publicado. 28-06-2024

N	RIESGO	Controles	Acciones Plan de Manejo	Evaluación	Observaciones frente al diseño y ejecución del Control y acciones del Plan de Manejo (Según Evidencias)
51	Posibilidad de que el servicio de impresión quede indisponible afectando la operación institucional.	El Administrador de infraestructura tecnológica monitorea trimestralmente el estado de los servidores de impresión, verificando disponibilidad y uso de recursos; conserva reportes y, ante fallas, activa la atención de incidentes y realiza seguimiento hasta su cierre.	Revisar trimestralmente la disponibilidad del servicio de impresión, analizar incidentes presentados y registrar acciones de mejora, siendo el responsable de la mesa de servicios (OTI).	100	Se observan evidencias de ejecución del control de manera trimestral con reportes de casos de la MDS resueltos y reportes de disponibilidad de activo

Fuente: Papel de trabajo evaluación riesgos SI

De acuerdo con las evidencias aportadas y la evaluación cualitativa, a continuación, se describen las situaciones encontradas de la evaluación de los controles sobre los riesgos identificados en la matriz de riesgos del proceso de TI y acciones del Plan de manejo:

Tabla N° 6. Resultados de Evaluación de Controles y Acciones					
N	RIESGO	Controles	Acciones Plan de Manejo	Evaluación	Observaciones frente al diseño y ejecución del Control y acciones del Plan de Manejo (Según Evidencias)
1	Posibilidad de afectación reputacional por incumplimiento en la implementación de los Planes y Proyectos de Tecnologías de la Información, debido al seguimiento inoportuno de las actividades propuestas.	La jefatura de la Oficina de Tecnologías de la Información (OTI), mensualmente realiza seguimiento a la ejecución de las actividades propuestas en los Planes y Proyectos de Tecnologías de la Información, reportando a su vez a la oficina de planeación el resultado de indicadores y cumplimiento de metas. Cuando se presenta incumplimiento en las metas o indicadores se debe reportar a la oficina de planeación un plan de mejora para evitar la materialización del riesgo. Registros: reporte de plan de acción, reporte de indicadores y planes de mejoramiento, si aplican.	"Entrega mensual del plan de acción y entrega trimestral de los indicadores del PETI a la Oficina Asesora de Planeación. Los planes de mejoramiento se desarrollarán únicamente cuando se presente incumplimiento en las metas o indicadores.	100	Se observa ejecución del control, en cuanto a proyecto de inversión y plan de acción; Mensualmente se realiza seguimiento y se remite a la Of de Planeación y trimestralmente se hace seguimiento a los indicadores del Plan Estratégico de Tecnología de la Información PETI. Se presenta además un informe cualitativo con el análisis de los resultados de indicadores de la OTI.
		El Comité Institucional de Gestión y Desempeño, anualmente revisa el avance de los Planes de Tecnología de la Información, en el cual se determinan las acciones a seguir para el cumplimiento de la implementación de las actividades realizadas y las modificaciones pertinentes. En caso de presentarse desviaciones en los resultados esperados, el comité tomará las decisiones necesarias para realizar acciones que puedan permitir el cumplimiento de los planes. Registro: actas de comité Institucional de Gestión y Desempeño	Registro: informe trimestral de la implementación del PETI durante la vigencia 2026"	95	"Se observa ejecución del control, en cuanto a la presentación de resultados del Plan Estratégico de Tecnología de la Información PETI, sin embargo, con el seguimiento de indicadores se hace de manera trimestral. Se observan seguimiento en Comité de Gestión y Desempeño.

 Agencia de Renovación del Territorio	INFORME		Código: FM-SEM-08
	SEGUIMIENTO EVALUACIÓN Y MEJORA		Versión: 05
	Grupo Interno de Trabajo de Control Interno		Publicado. 28-06-2024

N	RIESGO	Controles	Acciones Plan de Manejo	Evaluación	Observaciones frente al diseño y ejecución del Control y acciones del Plan de Manejo (Según Evidencias)
2	Posibilidad de afectación económica y reputacional por la falla servicios tecnológicos que detengan total o parcialmente la operación de la Agencia de Renovación del Territorio (ART), debido a eventos o incidentes de seguridad, mala implementación de servicios tecnológicos o por no tener en cuenta los controles establecidos por la Oficina de tecnología de la Información (OTI).	La Oficina de Tecnologías de la Información llevará a cabo trimestralmente el seguimiento a los controles de seguridad y tecnológicos. Este seguimiento se realizará mediante el uso de la herramienta de auto diagnóstico del Modelo de Seguridad y Privacidad de la Información durante el último mes de cada trimestre del año. Si se identifica alguna deficiencia en los controles, se procederá de inmediato a realizar los ajustes correspondientes necesarios para garantizar su efectividad y cumplimiento. Registro: Reporte de la herramienta de diagnóstico del modelo de seguridad y privacidad de la información.	Realizar Informe de disponibilidad de la plataforma en la herramienta Nagios, el cual deberá entregarse de manera trimestral el cual se debe entregar al grupo de gobierno Digital mediante correo electrónico. Registro: Informe de la Herramienta Nagios	80	Se encontró que la redacción de la actividad de control refiere el seguimiento de los controles a través del "Auto diagnóstico del Modelo de Seguridad y Privacidad de la Información durante el último mes de cada trimestre del año", sin embargo no se presenta registro del autodiagnóstico diligenciado. Se presenta lo referente al informe de NAGIOS mencionado en la acción del plan de manejo la cual es complementaria a la actividad de control por lo tanto no se evidencia ejecución del control para su calificación. AL respecto se reitera lo reportado a la Of. de Planeación "Esta herramienta permite supervisar de manera continua la plataforma tecnológica de la ART, facilitando la detección oportuna de eventos que puedan convertirse en incidentes o problemas y afectar la prestación de los servicios de TI. Adicionalmente, la herramienta proporciona una visión integral del estado de la infraestructura tecnológica, permitiendo conocer la disponibilidad y el estado de salud de la red, los servidores, las aplicaciones y demás componentes tecnológicos. Asimismo, genera alertas clasificadas como advertencias o críticas, de acuerdo con los umbrales definidos para cada uno de los activos monitoreados. Los resultados de este reporte son analizados por los profesionales responsables, quienes evalúan los eventos identificados y determinan las acciones que deban implementarse. Cuando se requiere realizar algún ajuste en la infraestructura tecnológica, este reporte sirve como insumo para la gestión y ejecución de los cambios correspondientes". No obstante, lo presentado en el seguimiento, esta actividad no reemplaza la ejecución del control. Se sugiere implementar la herramienta de autodiagnóstico establecida por MINTIC para la vigencia 2026 y/o ajustar el control de acuerdo a lo presentado y ejecutado como control. Se sugiere en la redacción de la actividad del control determinar el responsable no como una dependencia sino como el cargo de quien lo ejecuta o es responsable (Jefe de la OTI).
		La Oficina de Tecnologías de la Información diligenciará el formato de recibido a satisfacción cada vez que se realicen contratos con proveedores tecnológicos, además de gestionar la actualización de la documentación asociada a dichos contratos. Este proceso se llevará a cabo de manera inmediata, tras la finalización de cada contrato con proveedores tecnológicos. En caso de que no se reciba a satisfacción el servicio proporcionado por el proveedor, el supervisor del contrato de la Oficina de Tecnologías de la Información deberá solicitar al contratista los requerimientos necesarios para garantizar el cumplimiento a satisfacción del mismo. Registro: registro de recibido a satisfacción del servicio tecnológico y correo electrónico del supervisor de contrato al contratista (En caso de no recibir servicios a satisfacción)	Realizar Informes de supervisión e informes finales, de acuerdo con la modalidad del contrato. Estos documentos se entregarán según la finalización de cada contrato. A las personas encargadas de manejar el presupuesto de la Oficina de Tecnologías de la Información teniendo en cuenta los tiempos de ejecución de cada contrato. Registro: Informes de supervisión o informe final.	90	Se presentan los informes de supervisión de contratos, no obstante, se deben conservar en el repositorio de evidencias los registros de recibido a satisfacción del servicio tecnológico / correo electrónico del supervisor de contrato al contratista de servicios contratados con proveedores. Se informa que se tienen, pero no se encuentran disponibles en el repositorio de evidencias de ejecución de los controles, por lo cual se recomienda incluirlos. Se sugiere en la redacción de la actividad del control determinar el responsable no como una dependencia sino como el cargo de quien lo ejecuta o es responsable (Jefe de la OTI).

 Agencia de Renovación del Territorio	INFORME		Código: FM-SEM-08
	SEGUIMIENTO EVALUACIÓN Y MEJORA		Versión: 05
	Grupo Interno de Trabajo de Control Interno		Publicado. 28-06-2024

N	RIESGO	Controles	Acciones Plan de Manejo	Evaluación	Observaciones frente al diseño y ejecución del Control y acciones del Plan de Manejo (Según Evidencias)
3	Posibilidad de afectación económica y reputacional por insuficientes recursos financieros para la implementación y gestión del plan estratégico de tecnologías de la información y del sistema de gestión de seguridad de la información debido al mal diligenciamiento de la matriz de necesidades de la OTI y a falta de asignación presupuestal por parte de la ART.	La Jefatura de la Oficina de Tecnologías de la Información (OTI) solicitará anualmente a los funcionarios y contratistas de la dependencia sus necesidades en infraestructura tecnológica, seguridad de la información, gobierno digital, sistemas de información y soporte tecnológico. Estas serán documentadas en una matriz de necesidades para el periodo correspondiente. La solicitud se realizará a través de un correo electrónico anual dirigido al jefe de la oficina, quien lo remitirá al ordenador del gasto cuando este lo requiera. En caso de que no se asignen los recursos necesarios, se explorarán otras fuentes de financiación, como el Fondo Colombia en Paz, acuerdos o intercambios, los cuales serán evaluados según la necesidad. Registros: Matriz de necesidades diligenciada.	Elaborar la matriz de necesidades de los contratos que puedan realizarse a través del Fondo Colombia en Paz cuando no existan recursos del PGN y que permitan apalancar los proyectos del Plan Estratégico de Tecnologías de la Información y del Sistema de Seguridad y Privacidad de la Información, el cual es entregado a la Oficina de Planeación	85	La OTI consolidó y remitió las necesidades sobre el proyecto de inversión y gestión y se reportó por los correos a la Oficina de Planeación; se tiene la justificación del proyecto de inversión para el 2027; no obstante lo anterior, de acuerdo con lo descrito en la actividad de control no se observan registros y evidencias de ejecución "Matriz de necesidades diligenciada.". Es importante documentar la ejecución de esta actividad en lo corrido del primer semestre de 2026 y si se tuvieron que explorar otras fuentes de financiación por falta de asignación presupuestal para ejecutar lo planeado previamente para la vigencia 2026.
		La Oficina de Tecnologías de la Información gestionará anualmente la asignación de recursos necesarios ante las partes interesadas de la entidad, formalizando las necesidades ante la Secretaria General de la Agencia de Renovación del Territorio, quien es la responsable del proyecto de inversión de la Oficina de Tecnologías de la Información y del proyecto de funcionamiento de la Agencia de Renovación del Territorio. Esta gestión se realizará mediante la presentación de la matriz de necesidades de la Oficina de Tecnologías de la Información anualmente a la Secretaria General. Las necesidades aceptadas por la Secretaria General serán incluidas en el plan anual de adquisiciones. En caso de que alguna necesidad no sea aceptada, se clasificará como necesidades con déficit y se analizará la posibilidad de obtener recursos a través del Fondo Colombia en Paz. Registros: Acta de la sesión con secretaria general o agenda de invitación parte de la secretaria general para tratar el tema.	Registro: plan de adquisiciones.	80	Se sugiere en la redacción de la actividad del control determinar el responsable no como una dependencias sino como el cargo de quien lo ejecuta o es responsable (Jefe de la OTI). La OTI consolidó y remitió las necesidades sobre el proyecto de inversión y gestión y se reportó por los correos a la Oficina de Planeación; se tiene la justificación del proyecto de inversión para el 2027 y se tiene Plan de Adquisiciones de la vigencia 2026; no obstante lo anterior, de acuerdo a lo descrito en la actividad de control no se observan registros y evidencias de ejecución: "Matriz de necesidades diligenciada y Acta de la sesión con Secretaria General

 Agencia de Renovación del Territorio	INFORME		Código: FM-SEM-08
	SEGUIMIENTO EVALUACIÓN Y MEJORA		Versión: 05
	Grupo Interno de Trabajo de Control Interno		Publicado. 28-06-2024

N	RIESGO	Controles	Acciones Plan de Manejo	Evaluación	Observaciones frente al diseño y ejecución del Control y acciones del Plan de Manejo (Según Evidencias)
4	Posibilidad de afectación económica y reputacional para llevar a cabo la gestión ineficiente de los procesos y procedimientos de la Oficina de Tecnologías de la Información (OTI). debido a la insuficiente capacidad de recurso humano de la OTI y usuarios del sistema por deficiencias en la planeación de las capacitaciones requeridas	La Oficina de Tecnologías de la Información (OTI) verificará semestralmente que el GIT de Talento Humano incluya en el Plan Institucional de Capacitación (PIC) capacitaciones e inducciones requeridas para el personal de la OTI tendientes a cerrar brechas entre el entorno tecnológico actual y las habilidades y conocimientos del personal. En caso de requerir una capacitación específica no incluida en el PIC se solicitará al GIT de Talento Humano la inclusión de la misma. Registro: Matriz del PIC o correo electrónico con requerimiento de capacitación al GITTH.	Realizar semestralmente la solicitud de insumos para las capacitaciones de interés para la Oficina de Tecnologías de la Información. Registro: Envío del PIC con actividades de la Oficina de Tecnologías de la información.	90	Se sugiere en la redacción de la actividad del control determinar el responsable no como una dependencia sino como el cargo de quien lo ejecuta o es responsable (Jefe de la OTI). Si bien se tienen evidencias de solicitud al GIT de Talento Humano para incluir en el PIC las capacitaciones programadas por la OTI para la vigencia, el control se refiere a verificar que se incluyeron semestralmente, es decir que debería existir un registro de la verificación de que efectivamente el GIT de TH las incluyó e incluso que se ejecutaron, además de los establecidos.
		La Oficina de Tecnologías de la Información actualizará semestralmente la base de conocimiento en la aplicación de la mesa de servicios. Esta actualización garantiza que tanto usuarios como administradores de la infraestructura tecnológica puedan acceder a la información en línea en cualquier momento, fortaleciendo así sus conocimientos y facilitando su aprendizaje continuo. Además, se asegurará de que esta acción se refleje también en el repositorio de información de la Oficina de Tecnologías de la Información en el SharePoint. En caso de algún fallo de la plataforma y no se pueda realizar la publicación de la información se dispondrá de una herramienta alterna para su consulta y se informará a los funcionarios la forma en la cual podrán acceder. Registro: Captura de pantalla del repositorio de la mesa de servicios y de repositorio de la OTI en el servidor Mercurio, donde se aprecien las fechas de actualización.	Realizar semestralmente el monitoreo a la base de conocimiento de la mesa de servicios y actualizarla según lo consideren necesario los ingenieros de la mesa de servicios. Registro: reporte de la herramienta con corte al trimestre el cual se dejará en consulta en la misma herramienta.	75	Se sugiere en la redacción de la actividad del control determinar el responsable no como una dependencia sino como el cargo de quien lo ejecuta o es responsable (Jefe de la OTI). Se observan debilidades en la redacción del control lo cual es indicativo de una actividad de control en cuanto al uso de verbos y ejecución referida a verificaciones, comparaciones, revisiones, validaciones, monitorear, etc (entre otros verbos rectores); actualizar no es indicativo de una actividad de control dado que no permite identificar desviaciones, en este caso las referidas a "En caso de algún fallo de la plataforma y no se pueda realizar la publicación de la información se dispondrá de una herramienta alterna para su consulta y se informará a los funcionarios la forma en la cual podrán acceder", en cambio si lo sería verificar la aplicación de conocimientos en la mesa de servicios (por ejemplo). Por las inconsistencias de descripción o redacción del control, resulta no siendo claro el resultado plasmado en evidencias "Registro: Captura de pantalla del repositorio de la mesa de servicios y de repositorio de la OTI en el servidor Mercurio, donde se aprecien las fechas de actualización." Se hace la claridad de que es: el ingeniero responsable de la mesa de servicios que revisa la actualización permanente de la información y documentación de consulta disponible en la plataforma con el propósito de mantener el conocimiento organizado, vigente y accesible para todos los colaboradores (funcionarios/contratistas) que cuentan con acceso a la MDS. Se sugiere revisar además la redacción del riesgo si efectivamente sería "llevar a cabo una gestión ineficiente" y su coherencia con las actividades plasmadas de acuerdo a lo conversado y analizado en la reunión de seguimiento con el delegado de la OTI para la evaluación de este mapa de riesgos.

8. OPORTUNIDADES DE MEJORAMIENTO		
A continuación, se relacionan los HALLAZGOS identificados con la letra “H” y las OBSERVACIONES identificadas con la letra “O”		
Nº	TIPO	DESCRIPCIÓN
1	O	Debilidades en diseño, ejecución y evidencia de Actividades de Control de riesgos Se observan debilidades en el diseño, ejecución y documentación de 22 controles evaluados en niveles <i>REGULAR</i>, <i>ADECUADO</i> y <i>SATISFACTORIO</i> correspondientes a los Riesgos de Seguridad de la Información, sobre los cuales se presentan las observaciones al detalle en el numeral 7.2 – tabla 5 que, no de no ajustarse ni registrar evidencias en el repositorio, se podría generar una deficiente gestión de las desviaciones por falta de análisis y soporte de las acciones posteriores de mitigación. Asimismo, esta situación ocasiona el incumplimiento de la Guía para la Gestión Integral del Riesgo en Entidades Públicas (Versión 7), afectando la efectividad de los controles para el logro de los objetivos. Esta debilidad se ve reflejada de igual manera en el Mapa de Riesgos del Proceso de Tecnología de la Información, donde 6 de 8 controles evaluados (75%) presentan deficiencias en su diseño y ejecución detalladas en la Tabla 6 de este informe.
2	O	Duplicidad metodológica entre Actividades de Control y Planes de Manejo. Se observa que en la matriz de riesgos de Seguridad de la Información (formato FM-TI-36.V2), las acciones del plan de manejo en 22 ítems son idénticas de fondo a las actividades de control establecidas en cuanto a su ejecución y no define las acciones a seguir para priorizar los tratamientos de acuerdo con el impacto del riesgo residual conforme a lo descrito en el manual de política de riesgos de la ART (POL-DE-08 V1.2024) <i>“El tratamiento de los riesgos involucra identificar las opciones para tratar los riesgos residuales priorizados, con el fin de optimizar los recursos disponibles y enfocar los esfuerzos institucionales, la ART establece como prioridad el tratamiento de los riesgos de seguridad digital ubicados en las zonas de riesgo altas y extremas “</i> y no menciona que la acción del plan de manejo (columna AS) sea la misma acción descrita como control (columna Y). La Guía de Riesgos del DAFP-V7 define las acciones del plan de manejo como un <i>Plan de Acción o Tratamiento</i>, al duplicar la actividad de control, se está inobservando la estructura de la Tabla 30, la cual refiere una "Fecha de Implementación" única (un hito final) y no una periodicidad permanente (mensual, trimestral, etc); la guía se refiere a que el tratamiento busca <i>modificar</i> el riesgo, no repetir lo que ya existe. Con lo anterior, <i>una vez que el plan de tratamiento se haya ejecutado en las fechas y con las disposiciones de recursos previstas, se debe valorar nuevamente el riesgo y verificar si el nivel disminuyó o no, compararlo con el último nivel de riesgo residual⁹ con el fin de determinar si las acciones fueron efectivas.</i>
9. RECOMENDACIONES		
Revisar las observaciones descritas en las tablas 5 y 6 del presente informe para aplicar los correctivos necesarios al diseño, ejecución y documentación de los controles deficientes, garantizando el cumplimiento de la <i>Guía para la Gestión Integral del Riesgo en Entidades Públicas</i>. Para ello, el equipo de Seguridad de la Información deberá asegurar la completitud y suficiencia de los soportes en el repositorio institucional; esta gestión no debe limitarse exclusivamente a la información enunciada en la columna AW del formato, sino que requiere una lectura e interpretación integral del diseño del control y su respectivo análisis de desviaciones. En consecuencia, el equipo		

⁹ Guía de orientación para la gestión de riesgos de seguridad digital en el Gobierno Nacional, Territoriales y Sector Público.

 Agencia de Renovación del Territorio	INFORME	Código: FM-SEM-08
	SEGUIMIENTO EVALUACIÓN Y MEJORA	Versión: 05
	Grupo Interno de Trabajo de Control Interno	Publicado. 28-06-2024

deberá verificar que la evidencia recopilada corresponda plenamente a la naturaleza y alcance de la actividad de control descrita. En los casos donde la columna AW del formato FM-TI-36.V2 presente omisiones o sea insuficiente para respaldar la ejecución real del control, se deberá ajustar y complementar la descripción técnica de los soportes requeridos para mitigar oportunamente las desviaciones identificadas.

- Ajustar la Matriz de Riesgos de Seguridad de la Información (formato FM-TI-36.V2), eliminando la duplicidad entre las actividades de control (columna Y) y las acciones del plan de manejo (columna AS). Para ello, el equipo de seguridad de la Información deberá redefinir las acciones de los planes de manejo con un hito o fecha de implementación única orientados a modificar el riesgo y no a repetir controles permanentes, en cumplimiento de la Tabla 30 de la *Guía de Riesgos del DAFP (Versión 7)*. Lo anterior en alineación con el Manual de Política de riesgos de la ART priorizando las opciones de tratamiento para los riesgos residuales ubicados en las zonas de riesgo inherente alta y extrema. Una vez ejecutados las acciones definidas en el plan dentro de los plazos previstos, se deberá realizar una nueva valoración del riesgo para medir la efectividad de las acciones frente al último nivel de riesgo residual.

10. CONCLUSIONES

Se evaluó el diseño y ejecución de los controles de los Riesgos del Proceso de TI y de Seguridad de la Información, así como las acciones definidas en los planes de tratamiento, encontrando que tanto los controles como los planes de manejo se encuentran en ejecución.

Sobre la muestra evaluada se verificó el diseño y ejecución de los controles a partir de los criterios definidos en la metodología con el fin de determinar si son adecuados para evitar la materialización de riesgos y, a partir de la muestra definida, se determina que en promedio la evaluación de los controles de Seguridad de la Información se ubican en un nivel **SATISFACTORIO** con una calificación de nivel 91/100 (el 56% de ellos en un nivel óptimo de diseño y ejecución) y, la evaluación de los controles del Mapa de riesgos del proceso de Tecnología de la Información arroja un consolidado promedio de 87/100 ubicándose en un nivel **ADECUADO**, con observaciones que requieren una revisión de fondo.

Se verificó que se lleva a cabo el seguimiento periódico a la ejecución de los controles y acciones del plan de manejo de riesgos por parte del equipo de seguridad de la Información de la OTI como segunda línea de defensa sobre el Mapa de Riesgos de Seguridad de la Información, sin embargo, se debe mejorar la organización del repositorio de evidencias considerando que la principal debilidad consiste en la conservación y documentación de las mismas.

11. FIRMAS RESPONSABLES

Auditor: 	Vo. Bo MARLON SALOMON CONTRERAS TURBAY  Firmado digitalmente por MARLON SALOMON CONTRERAS TURBAY Fecha: 2026.09.07 15:39:11 -05'00'
NOMBRE: MARISOL GUTIERREZ HERNANDEZ CARGO: CONTRATISTA GITCI	NOMBRE: MARLON SALOMON CONTRERAS TURBAY CARGO: Coordinador GIT de Control Interno
FECHA DE INFORME:	31 de Agosto de 2026