

 Empresa Nacional Promotora del Desarrollo Territorial S.A.	INFORME DE SEGUIMIENTO Y EVALUACIÓN (Trabajos de informes, seguimientos de ley y/o cumplimiento)	CÓDIGO:	F-AU-10
		VERSIÓN:	04
		VIGENCIA:	2025-06-12
	AUDITORÍA INTERNA	CLASIFICACIÓN:	IP

N.º 43

EMPRESA NACIONAL PROMOTORA DEL DESARROLLO TERRITORIAL S.A

ASESORIA DE CONTROL INTERNO

**INFORME SEGUIMIENTO A LAS OBLIGACIONES CONTRACTUALES DEL CONTRATISTA
EN MATERIA DE SERVICIOS DE SEGURIDAD TECNOLÓGICA (ANEXO NO. 2, Contrato No.
2024612 INA-007-2024)**

**PERIODO EVALUADO:
JULIO 2025 A JULIO DE 2026**

**Elaborado:
SEPTIEMBRE DE 2026**

 Empresa Nacional Promotora del Desarrollo Territorial S.A.	INFORME DE SEGUIMIENTO Y EVALUACIÓN (Trabajos de informes, seguimientos de ley y/o cumplimiento)	CÓDIGO:	F-AU-10
		VERSIÓN:	04
		VIGENCIA:	2025-06-12
	AUDITORÍA INTERNA	CLASIFICACIÓN:	IP

CONTENIDO

INFORMACIÓN GENERAL:	3
DESARROLLO DEL INFORME:	3
OBJETIVO	3
ALCANCE	3
LIMITACION DEL ALCANCE (SI APLICA)	4
MARCO LEGAL	4
RESULTADOS DEL SEGUIMIENTO	5

 Empresa Nacional Promotora del Desarrollo Territorial S.A.	INFORME DE SEGUIMIENTO Y EVALUACIÓN (Trabajos de informes, seguimientos de ley y/o cumplimiento)	CÓDIGO:	F-AU-10
		VERSIÓN:	04
		VIGENCIA:	2025-06-12
	AUDITORÍA INTERNA	CLASIFICACIÓN:	IP

INFORMACIÓN GENERAL:

NOMBRE DEL INFORME:	<i>INFORME SEGUIMIENTO A LAS OBLIGACIONES CONTRACTUALES DEL CONTRATISTA EN MATERIA DE SERVICIOS DE SEGURIDAD TECNOLÓGICA (ANEXO NO. 2, INA-007-2024)</i>
TIPO DE INFORME:	<i>Informe de seguimiento</i>
DESTINATARIOS:	<i>Armando Vivas Salamanca Gerente Tecnologías de la Información</i>
FUENTE DE INFORMACIÓN:	<i>Gestión de Tecnologías de la Información</i>
EMITIDO POR:	<i>Orlando Correa Núñez</i>
AUDITOR:	<i>Luisa Fernanda Ríos Giraldo</i>

DESARROLLO DEL INFORME:

OBJETIVO

Verificar el cumplimiento de las obligaciones contractuales del Contratista en materia de Servicios de Seguridad Tecnológica (Anexo No. 2, Contrato No. 2024612 INA-007-2024), conforme a ISO 27001:2022, identificando el grado de implementación real de los controles, el cumplimiento de los ANS pactados y la existencia de evidencia documental que soporte la operación continua y segura de la plataforma tecnológica de la Sociedad.

ALCANCE

Verificar el cumplimiento de las obligaciones contractuales del Contratista en materia de Servicios de Seguridad Tecnológica (Anexo No. 2, Contrato No. 2024612 INA-007-2024). La evaluación independiente cubre los 2 dominios priorizados por su nivel de criticidad: D01 – Controles de Seguridad Base, y D04 – SOC/SIEM, así como el cumplimiento de las funciones del supervisor del contrato como segunda línea de aseguramiento.

La verificación se efectuó con los soportes documentales de la ejecución del contrato en el periodo comprendido entre julio de 2025 y julio de 2026.

	INFORME DE SEGUIMIENTO Y EVALUACIÓN (Trabajos de informes, seguimientos de ley y/o cumplimiento)	CÓDIGO:	F-AU-10
		VERSIÓN:	04
		VIGENCIA:	2025-06-12
	AUDITORÍA INTERNA	CLASIFICACIÓN:	IP

LIMITACIÓN DEL ALCANCE

No se identificaron limitaciones al alcance del seguimiento.

MARCO LEGAL

El presente seguimiento de cumplimiento al Contrato INA-007-2024, Anexo Técnico No. 2 – Servicios de Seguridad Tecnológica, se fundamenta en el siguiente marco normativo:

En materia contractual, los artículos 13 y 15 de la Ley 1150 de 2007 "Por medio de la cual se introducen medidas para la eficiencia y la transparencia en la Ley 80 de 1993 y se dictan otras disposiciones generales sobre la contratación con Recursos Públicos", que establecen que ENTerritorio S.A, en su calidad de Empresa Industrial y Comercial del Estado de carácter financiero (Decreto 495 de 2019), se rige por el derecho privado cuando actúa como contratante; en consecuencia, las normas que gobiernan el Contrato INA-007-2024 son el Código Civil (arts. 1494 y ss., en materia de obligaciones y cumplimiento), el Código de Comercio (arts. 822 y ss., contratos mercantiles y sus obligaciones) y el Estatuto Orgánico del Sistema Financiero, aplicable por la naturaleza jurídica de la entidad. El proceso de selección y la ejecución del contrato se rigen adicionalmente por el Manual de Contratación M-PR-01 v2 de ENTerritorio S.A, aprobado mediante Acuerdo de Junta Directiva No. 292 del 16 de octubre de 2020 (Numeral 28 – Invitación Abierta – INA), y el Decreto 1082 de 2015 "Decreto Único Reglamentario del Sector Administrativo de Planeación Nacional" se aplica de manera supletoria en los principios de la contratación y en la obligación de publicación en SECOP II (art. 2.2.1.2.1.1).

Ley 1474 de 2011 "Estatuto Anticorrupción" (arts. 83, 84 y 85, sobre deberes, facultades y responsabilidad del supervisor contractual).

El Decreto 1082 de 2015 "Decreto Único Reglamentario del Sector Administrativo de Planeación Nacional" (arts. 2.2.1.1.1.6.1, 2.2.1.2.1.1 y 2.2.1.2.4.4, relativos a la supervisión, principios de la contratación y acuerdos de niveles de servicio en contratos de TI).

En el ámbito de la auditoría interna, aplican las Normas Globales de Auditoría Interna™ – NOGAI (IIA, 2024, vigentes desde enero de 2025), Principios 13 (estándares 13.1 a 13.4: planificación, programa de trabajo y supervisión del trabajo), 14 (obtención y documentación de evidencia) y 15 (comunicación de resultados), en concordancia con el Procedimiento de Auditorías de Gestión y Trabajos de Aseguramiento P-AU-01 v6 (vigente desde el 12 de junio de 2025) y la Guía para la Gestión Estratégica y el Fortalecimiento de la Auditoría Interna del DAFP, versión 5 (julio de 2026).

En materia de seguridad de la información y tecnología, el Anexo Técnico No. 2 establece como criterios de evaluación obligatorios la norma ISO/IEC 27001:2022 "Sistemas de Gestión de Seguridad de la Información – Requisitos" (cláusulas 6.1, 8.1, 9.1 y 10, y Anexo A controles A.5, A.8, A.5 y A.8).

A nivel interno, constituyen criterios de cumplimiento la Política Institucional de Seguridad de la Información ORI-01 v4, el Procedimiento de Gestión de Incidentes P-RI-19 v4 y los documentos del Sistema Integrado de Gestión de ENTerritorio S.A.

En materia de protección de datos personales, aplica la Ley 1581 de 2012 "Por la cual se dictan disposiciones generales para la protección de datos personales" (arts. 4, 17, 18, 19 y 26), reglamentada

	INFORME DE SEGUIMIENTO Y EVALUACIÓN (Trabajos de informes, seguimientos de ley y/o cumplimiento)	CÓDIGO:	F-AU-10
		VERSIÓN:	04
		VIGENCIA:	2025-06-12
	AUDITORÍA INTERNA	CLASIFICACIÓN:	IP

por el Decreto 1074 de 2015, dado que el contratista accede y trata información personal de servidores y usuarios de la entidad en el marco de la prestación de los servicios objeto de seguimiento.

RESULTADOS DEL SEGUIMIENTO

Antecedente del tema a evaluar

El Anexo Técnico No. 2 - Servicios de Seguridad Tecnológica constituye uno de los 9 componentes del Contrato No. 2024612 (INA-007-2024), con vigencia del 27 de mayo de 2024 al 26 de mayo de 2027.

Dicho anexo describe las condiciones técnicas bajo las cuales el Contratista debe proveer, implementar, administrar y mantener los controles y servicios de ciberseguridad sobre la plataforma tecnológica de la Entidad, la cual opera en 4 entornos: Centro de Datos Principal en modalidad IaaS (CCP), Centro de Datos Alternativo en modalidad IaaS (CCA), Centro de Comunicaciones Básico propiedad de ENTerritorio S.A (CCB – Calle 26 No. 13-19) y Sede Archivo Central Histórico (ACH – Calle 12 No. 79a-25), con proyección a nube pública Azure.

El Anexo No. 2 desarrolla 13 componentes de servicio:

- i) Implementación, administración y monitoreo de controles de seguridad, incluyendo hardening, gestión de vulnerabilidades, análisis de parches con mecanismo de rollback y gestión de identidades (SSO, MFA, Directorio Activo);
- ii) Servicios de seguridad para networking (firewall NGFW/HA, NAC, IPS/IDS, SD-WAN, VPN, segmentación de redes, portales cautivos);
- iii) Centro de Operaciones de Seguridad SOC en modalidad 7x24x365, con correlación de eventos (SIEM, mínimo 1.000 EPS o 100 dispositivos, retención mínima de 6 meses) y análisis forense (ISO/IEC 27037);
- iv) Servicios de certificados digitales (SSL/TLS 1.2+, Wildcard, SSO, telefonía);
- v) Antimalware/EDR;
- vi) Prevención de pérdida de datos (DLP);
- vii) Control de acceso a la red (NAC, 750-1.000 usuarios promedio);
- viii) Seguridad web (WAF, protección DoS, OWASP Top 10);
- ix) Suministro y administración de equipos firewall para CCB y ACH;
- x) Acuerdos de Nivel de Servicio (ANS) con disponibilidad mínima exigida del 99,98 % para todos los componentes, con penalidades escalonadas (10 % a 100 % de descuento sobre facturación);
- xi) ANS de Impacto Operativo con escala de criticidad insignificante–catastrófico (ISO 27035);

	INFORME DE SEGUIMIENTO Y EVALUACIÓN (Trabajos de informes, seguimientos de ley y/o cumplimiento)	CÓDIGO:	F-AU-10
		VERSIÓN:	04
		VIGENCIA:	2025-06-12
	AUDITORÍA INTERNA	CLASIFICACIÓN:	IP

xii) Transición de entrada en operación (Anexo No. 9); y

xiii) Transición, cierre y entrega.

Mediante la Adenda No. 01 de fecha 1.º de marzo de 2024 y el Memorando de Alcance F-PR-26 del 26 de febrero de 2024, suscritos por el Gerente GTI y el Subgerente Administrativo, se introdujeron precisiones a los numerales 6 (Antimalware/EDR) y 7 (DLP) del Anexo No. 2, ampliando la cobertura a nube, Outlook y ERP, así como 19 obligaciones específicas del Contratista para la línea de seguridad, entre las que se destacan la obligación de cumplir con las normas ISO 27001 e ISO 27000, coadyuvar en los procesos de seguimiento y recertificación, garantizar el acceso a consolas de administración al Supervisor del Contrato y entregar informes de gestión mensuales.

La versión consolidada del Anexo No. 2 según Adenda No. 1, es el documento de referencia normativa vigente para efectos del presente ejercicio de seguimiento.

Priorización definida para el seguimiento

En atención a los criterios de riesgo, relevancia y materialidad establecidos en las Normas Globales de Auditoría Interna (NOGAI 2024) del IIA (principios 13 a 15), la Asesoría de Control Interno focalizó esta evaluación independiente en 2 dimensiones del Anexo No. 2, identificadas como de mayor riesgo operativo y e impacto potencial sobre la continuidad de los servicios tecnológicos de ENTerritorio S.A: D01 – Controles de Seguridad Base (hardening, gestión de vulnerabilidades y pentesting) y D04 – SOC/SIEM/Monitoreo/Análisis Forense, así como el cumplimiento de las obligaciones por parte del supervisor del Anexo.

La priorización responde a las siguientes consideraciones:

a) D01, agrupa las obligaciones de carácter preventivo más críticas (plantillas de hardening, ciclos de parches con rollback, herramienta de gestión de vulnerabilidades y pentesting anual por tercero certificado), cuya ausencia o deficiencia compromete la seguridad de la plataforma,

b) D04, concentra el mayor componente de operación continua contratada (SOC 7×24×365 con SIEM centralizado), con incidencia directa sobre el ANS de disponibilidad ($\geq 99,98\%$), las penalidades por impacto operativo y el cumplimiento del Procedimiento P-RI-19 v4 de Gestión de Incidentes de ENTerritorio S.A

Los demás componentes del Anexo No. 2 (certificados digitales, antimalware/EDR, DLP, NAC, seguridad web y suministro de equipos firewall CCB/ACH) hacen parte del universo auditable del contrato y podrán ser objeto de evaluaciones complementarias en ejercicios posteriores, sin que su exclusión del presente informe signifique conformidad con su ejecución.

A continuación se presenta el detalle de los dominios priorizados:

 Empresa Nacional Promotora del Desarrollo Territorial S.A.	INFORME DE SEGUIMIENTO Y EVALUACIÓN (Trabajos de informes, seguimientos de ley y/o cumplimiento)	CÓDIGO:	F-AU-10
		VERSIÓN:	04
		VIGENCIA:	2025-06-12
	AUDITORÍA INTERNA	CLASIFICACIÓN:	IP

Tabla 1 Priorización del seguimiento

N.º	Componente / Dimensión	Descripción y Obligaciones Principales	Norma / Marco Aplicable
2	D01 – Controles de Seguridad Base	Hardening de equipos y sistemas (configuración segura) Gestión de vulnerabilidades técnicas Gestión de parches con procedimiento de rollback Gestión de identidades: SSO y MFA Seguridad en IaaS (CCP y CCA)	ISO 27001:2022, Anexo A: A.8.8 – Gestión vulnerabilidades técnicas A.8.9 – Gestión configuración (hardening) A.5.37 – Documentación de procedimientos de operación A.8.2 – Derechos de acceso privilegiado NOGAI 2024 – Principios 13 a 15
5	D04 – SOC / SIEM / Monitoreo / Análisis Forense	SOC 7×24×365 con personal calificado SIEM: mínimo 1.000 EPS o 100 dispositivos monitoreados Correlación de eventos e inteligencia de amenazas Retención de logs: mínimo 6 meses Análisis forense digital: mínimo 2 análisis/año Gestión y respuesta a incidentes de seguridad	ISO 27001:2022, Anexo A: A.8.15 – Registro de eventos (logging) A.8.16 – Actividades de monitoreo ISO/IEC 27035:2023 – Gestión de incidentes de SI ISO/IEC 27037:2012 – Evidencias digitales NOGAI 2024 – Principios 13 a 15
★	Seguimiento a Obligaciones del Supervisor Contractual	Supervisor: Armando Vivas Salamanca (Gerente GTI - ENTerritorio) Verificar el cumplimiento de las funciones de supervisión conforme al Manual M-PR-01 v2: · Revisión y aprobación de informes del contratista · Control de ANS (disponibilidad e impacto operativo) · Registro y seguimiento de actas de seguimiento · Gestión de incidentes y aplicación de penalidades · Verificación de obligaciones técnicas y laborales del contratista	M-PR-01 v2 – Manual de Supervisión Contractual ENTerritorio Estatuto General de Contratación (Ley 80/1993, Art. 84) NOGAI 2024 – Principios 13 a 15 (criterios de riesgo, relevancia y materialidad) Contrato No. 2024612 – Cláusulas de supervisión

Verificación técnica de los criterios

Con el propósito de dar inicio formal a la recopilación de evidencias, la Asesoría de Control Interno remitió al Grupo de Tecnologías de la Información (GTI) el Memorando No. 202611010004483 del 3 de septiembre de 2026, mediante el cual se formuló la solicitud de información correspondiente al período de evaluación comprendido entre julio de 2025 y julio de 2026, con plazo de respuesta hasta el 9 de septiembre de 2026.

Dicha solicitud comprendió los requerimientos informativos asociados a la dimensión D01 – Controles de Seguridad Base (soportes de hardening, reportes de escaneo de vulnerabilidades, informe de pentesting, ciclos de parches, inventario de dispositivos y plan de mejoramiento), la dimensión D04 – SOC / SIEM / Monitoreo / Análisis Forense (fuentes conectadas al SIEM, reglas de correlación, monitoreo 7×24×365,

	INFORME DE SEGUIMIENTO Y EVALUACIÓN (Trabajos de informes, seguimientos de ley y/o cumplimiento)	CÓDIGO:	F-AU-10
		VERSIÓN:	04
		VIGENCIA:	2025-06-12
	AUDITORÍA INTERNA	CLASIFICACIÓN:	IP

tickets de incidentes, informes forenses y tiempos de respuesta vs. ANS), así como los elementos relacionados con la supervisión contractual del GTI conforme al Manual M-PR-01 v2.

Una vez recibida la información aportada por el Grupo GTI, la Asesoría de Control interno procedió a su revisión documental, y de la cual se llevó a cabo una mesa de trabajo el día lunes 14 de septiembre de 2026, con la participación del Gerente del Grupo TI, oficial de seguridad (supervisor del Anexo No. 2) y el proveedor del contrato, con el fin de socializar el estado de verificación de los criterios evaluados, clarificar los aspectos técnicos pertinentes e identificar las evidencias pendientes de aporte.

En continuidad con dicha reunión, mediante Memorando No. 202611010004833 del 15 de septiembre de 2026, se remitió al Grupo GTI la *Matriz de Verificación D01_D04 SecciónIII (Copia Gerencia TI_D01_D04 SeccionIII_20260915.xlsx)*, la cual contiene el estado consolidado de verificación con corte al 14 de septiembre de 2026, precisando los criterios con resultado Cumple Parcial y No Aportado que requerían complementación, a excepción de los criterios D04-6 (informes de análisis forense) y III.2 (requerimientos formales escritos del supervisor al contratista), que contaban con justificación formal por parte de GTI a través del Memorando No. 202615010002183 del 9 de septiembre de 2026; el plazo para la remisión de evidencias complementarias y el diligenciamiento de la columna de aclaraciones técnicas se fijó hasta el 17 de septiembre de 2026.

Frente al criterio D04-6, el GTI certificó que durante el período de evaluación comprendido entre julio de 2025 y julio de 2026 no se presentó ni se materializó ningún incidente de seguridad de la información de criticidad Moderada, Mayor o Catastrófica en la plataforma tecnológica de la Sociedad.

En consecuencia, manifestó que los informes de análisis forense y los registros de cadena de custodia asociados no fueron requeridos ni generados en la operación real, por cuanto el Anexo Técnico No. 2 establece que dicho servicio se activa bajo demanda únicamente para los casos en que sea necesario investigar incidentes informáticos.

Frente al criterio III.2, relativo a la existencia de requerimientos formales escritos dirigidos al contratista, el GTI precisó que, la supervisión técnica se ha ejercido de manera continua y documentada a través de las actas de seguimiento suscritas cada 8 días, las cuales concentran el desarrollo de las 8 líneas del contrato y han constituido el mecanismo de seguimiento desde el inicio de la ejecución contractual.

Por lo anterior, la Asesoría de Control Interno registró esta aclaración como justificación formal del GTI y procedió a verificar que las actas de seguimiento aportadas por el área, cubran el registro de los compromisos, requerimientos y novedades técnicas del Anexo Técnico No. 2, con el fin de establecer si dicho mecanismo satisface los requisitos de trazabilidad de supervisión exigidos por el Manual M-PR-01 v2 y las obligaciones contractuales del supervisor.

 Empresa Nacional Promotora del Desarrollo Territorial S.A.	INFORME DE SEGUIMIENTO Y EVALUACIÓN (Trabajos de informes, seguimientos de ley y/o cumplimiento)	CÓDIGO:	F-AU-10
		VERSIÓN:	04
		VIGENCIA:	2025-06-12
	AUDITORÍA INTERNA	CLASIFICACIÓN:	IP

Desarrollo de la verificación por la Asesoría de Control Interno

- Dominio D01:

Tabla 2 Obligaciones principales del Dominio 01

N.º	Componente / Dimensión	Descripción y Obligaciones Principales	Norma / Marco Aplicable
2	D01 – Controles de Seguridad Base	Hardening de equipos y sistemas (configuración segura) Gestión de vulnerabilidades técnicas Gestión de parches con procedimiento de rollback Gestión de identidades: SSO y MFA Seguridad en IaaS (CCP y CCA)	ISO 27001:2022, Anexo A: A.8.8 – Gestión vulnerabilidades técnicas A.8.9 – Gestión configuración (hardening) A.5.37 – Documentación de procedimientos de operación A.8.2 – Derechos de acceso privilegiado NOGAI 2024 – Principios 13 a 15

- D01-1

Criterios: ISO/IEC 27001:2022

C.8.9 – Gestión de configuración segura

C.5.37 – Documentación de procedimientos

Criterio de verificación (Anexo Técnico No. 2):

*“El Contratista debe realizar el hardening **previo** a la entrada en producción de los siguientes componentes: Sistemas operativos (servidores y estaciones de usuarios), Virtualizadores, Bases de datos, Software y servidores de aplicaciones, Sistemas en nube pública, Sistemas de enrutamiento y conmutación, Circuito Cerrado de Seguridad.*

El Contratista debe presentar las plantillas de hardening para cada sistema. Estas deben ser aprobadas por el supervisor del contrato.

El Contratista debe realizar una revisión periódica en todos los sistemas de las políticas de hardening implementadas y presentar un informe con las recomendaciones de mejora.”

En atención al requerimiento de convalidación (Memorando No. 202615010002213 del 17-09-2026), GTI allegó, para el criterio D01-1, el siguiente conjunto de evidencias:

- i) 4 informes de escaneo OWASP ZAP by Checkmarx v2.17.0 (PT-D01-1-E1 a E4),
- ii) 4 Actas de Comité de Cambios de Infraestructura No. 03, 12, 13 y 14 de 2026 (PT-D01-1-E5 a E8), y
- iii) El documento “Evidencias Cambios Parchado”, que consolida 19 casos de cambio registrados y cerrados en la herramienta ARANDA (Cambios No. 2096 a 2470, PT-D01-1-E9).

En relación con la aplicación desplegada en la vigencia del contrato (el sistema "Formulario Operaciones Inusuales" (OPE_INUSUALES), accesible en los dominios roi.enterritorio.gov.co e internamente en

	INFORME DE SEGUIMIENTO Y EVALUACIÓN (Trabajos de informes, seguimientos de ley y/o cumplimiento)	CÓDIGO:	F-AU-10
		VERSIÓN:	04
		VIGENCIA:	2025-06-12
	AUDITORÍA INTERNA	CLASIFICACIÓN:	IP

172.16.x.xx), el análisis de los soportes documentales permitió reconstruir la siguiente secuencia operativa:

El Acta de Comité de Cambios No. 03 (05-02-2026, ítem A49 Extraordinario, Cambio 2323, PT-D01-1-E5) indicó que el aplicativo fue desplegado en el servidor de producción el 8 de enero de 2026. Con posterioridad al despliegue, el operador tecnológico realizó un escaneo de vulnerabilidades OWASP ZAP sobre el sitio roi.enterritorio.gov.co (16-01-2026, PT-D01-1-E1), el cual identificó 2 hallazgos de riesgo Alto (Redirección Externa (×14 instancias) y SQL Injection SQLite Time Based (×2 instancias)), resultados que fueron remitidos al desarrollador. Ante la persistencia de vulnerabilidades sin mitigar, la aplicación se mantuvo restringida a acceso exclusivo desde red interna o VPN, dándose cierre administrativo al ítem en dicho estado.

Sobre el aplicativo desplegado en 172.16.x.xx, el escaneo del 12-03-2026 (PT-D01-1-E2) detectó 2 hallazgos Altos (librería JavaScript vulnerable moment.js 2.15.2 (CVE-2017-18214, CVE-2022-24785) y Redirección Externa (×15)).

El escaneo del 20-03-2026 (PT-D01-1-E3) identificó 1 hallazgo ALTO (Redirección Externa (×30)) y hallazgos de riesgo MEDIO, entre ellos Directory Browsing y fuga de información mediante archivo .env.

El escaneo del 27-03-2026 (PT-D01-1-E4), realizado sobre los endpoints de Azure/Microsoft utilizados por la aplicación, arrojó 0 hallazgos de riesgo ALTO.

El Acta de Comité de Cambios No. 12 (16-04-2026, ítem A12, Cambio 2387, PT-D01-1-E6) aprobó la ejecución de ajustes a los servicios JavaScript y demás mitigaciones frente a las vulnerabilidades detectadas, la cual fue ejecutada satisfactoriamente el 17-04-2026 con un puntaje de seguridad reportado del 88%, conforme lo ratifica el Acta No. 13 (23-04-2026, PT-D01-1-E7).

Finalmente, el Acta No. 13 (ítem A13, Cambio 2390) aprobó la publicación externa del aplicativo ROI el 23-04-2026, con integración al WAF, y el Acta No. 14 (30-04-2026, PT-D01-1-E8) confirmó el cierre satisfactorio del cambio.

El documento de soportes documentales de cambios parchados (PT-D01-1-E9) consolidó adicionalmente 19 casos ARANDA de actualización y parchado de infraestructura (servidores, bases de datos, componentes de seguridad) en estado cerrado: "Cambio efectuado 465", lo cual permitió evidenciar la existencia de un proceso de gestión de cambios activo durante el período.

- Resultado del análisis documental:

Del análisis de los soportes documentales aportados, la Asesoría de Control Interno concluyó lo siguiente:

- i) El proveedor implementó un proceso iterativo de análisis de vulnerabilidades mediante OWASP ZAP sobre el sistema desplegado en la vigencia (OPE_INUSUALES), con 4 escaneos que documentan la progresiva reducción del nivel de riesgo hasta la eliminación de hallazgos ALTO previo a la publicación externa de la aplicación el 23-04-2026,

 Empresa Nacional Promotora del Desarrollo Territorial S.A.	INFORME DE SEGUIMIENTO Y EVALUACIÓN (Trabajos de informes, seguimientos de ley y/o cumplimiento)	CÓDIGO:	F-AU-10
		VERSIÓN:	04
		VIGENCIA:	2025-06-12
	AUDITORÍA INTERNA	CLASIFICACIÓN:	IP

- ii) Las actualizaciones de seguridad e infraestructura fueron sometidas a aprobación del Comité de Cambios, con evaluación de costos, riesgos y opción de rollback,
- iii) Los cambios indicados quedaron registrados en la herramienta ARANDA.
- iv) No obstante lo anterior, el criterio D01-1 exige adicionalmente la existencia de plantillas de hardening por sistema aprobadas por el supervisor del contrato, cuyo soporte documental no fue aportado en la convalidación ni se identificó en los documentos revisados; así como el informe de revisión periódica con resultados e identificación de oportunidades de mejora.

En consecuencia, la valoración del criterio D01-1 se identifica con **CUMPLIMIENTO PARCIAL**.

Las evidencias de convalidación aportadas por GTI el 17 de septiembre de 2026, confirman la existencia de un proceso activo de análisis y remediación de vulnerabilidades con herramienta OWASP ZAP y gestión formal de cambios, lo cual representa un avance sustancial respecto a las evidencias iniciales aportadas el 9 de septiembre de 2026; sin embargo, persiste la ausencia de plantillas de hardening aprobadas por sistema y de informes de revisión periódica con identificación de mejoras, elementos constitutivos del pleno cumplimiento del criterio conforme al Anexo Técnico No. 2.

- **D01-2**

Criterios: ISO/IEC 27001:2022

C.8.8 – Gestión de vulnerabilidades técnicas

Criterio de verificación (Anexo Técnico No. 2):

“GESTIÓN DE VULNERABILIDADES: El Contratista debe realizar la **detección, gestión y solución de vulnerabilidades en los siguientes componentes:** Sistemas operativos (servidores y estaciones), Virtualizadores, Bases de datos, Software y servidores de aplicaciones, Sistemas en nube pública, Sistemas de enrutamiento y conmutación, Circuito Cerrado de Seguridad. //

El CONTRATISTA **debe mitigar y solucionar las vulnerabilidades** encontradas en la plataforma tecnológica. Como valor de referencia se presenta un promedio de 400 vulnerabilidades por año.”

Con el propósito de verificar el cumplimiento de este criterio, la Asesoría de Control Interno revisó los soportes documentales aportados por GTI, correspondientes a dos componentes principales:

- i) Informes ejecutivos de análisis de vulnerabilidades técnicas elaborados mediante la herramienta Nessus Professional y formalizados en el Formato F-RI-25 "Análisis y Remediación de Vulnerabilidades Técnicas", y
- ii) 7 Informes mensuales de monitoreo SOC producidos por el Centro de Operaciones de Seguridad durante el período comprendido entre el 27 de diciembre de 2025 y el 26 de julio de 2026.

 Empresa Nacional Promotora del Desarrollo Territorial S.A.	INFORME DE SEGUIMIENTO Y EVALUACIÓN (Trabajos de informes, seguimientos de ley y/o cumplimiento)	CÓDIGO:	F-AU-10
		VERSIÓN:	04
		VIGENCIA:	2025-06-12
	AUDITORÍA INTERNA	CLASIFICACIÓN:	IP

- **Análisis por eje de criterio:**

ESCANEOS DE VULNERABILIDADES Y FORMATO F-RI-25

Respecto al componente de análisis de vulnerabilidades, se verificaron 2 escaneos ejecutados con Nessus Professional sobre la infraestructura tecnológica de Enterritorio S.A:

- I) El primero, correspondiente al entorno de Pruebas/CCA, cubrió 64 hosts distribuidos en 5 segmentos de red, identificando 2.651 vulnerabilidades, de las cuales 420 fueron clasificadas como Críticas (15,8%), 483 como Altas (18,2%) y 1.659 como Medias (62,6%), con registro de 1.856 CVE asociados.
- II) El segundo escaneo, ejecutado el 27 de junio de 2026 sobre el entorno de Producción CCP, cubrió 79 hosts e identificó 12.310 vulnerabilidades, con una distribución de 3.296 Críticas (26,8%) y 3.650 Altas (29,6%). De estas últimas, 10.814 (equivalentes al 87,8% del total) se concentran en siete (7) servidores Oracle Database (172.16.x.xxx a 172.16.x.xxx), asociadas a vulnerabilidades en Oracle Java SE, Apache Tomcat y Log4j.

De acuerdo a los soportes documentales, para la gestión de los hallazgos, el contratista implementó un esquema de planes de remediación diferenciados por criticidad: P0 (corrección en 7 días), P1 (15 días), P2 (30 a 60 días) y P3 (90 días), conforme a lo establecido en el Anexo Técnico No. 2.

No obstante, en la verificación documental, el análisis de las matrices F-RI-25 refleja tasas de remediación bajas: En el entorno de Pruebas/CCA se cerraron 340 de 2.651 vulnerabilidades (12,8%), mientras que en el entorno de Producción CCP, 446 de 12.310 (3,6%) fueron cerradas, con 6.202 en estado "Sin Remediación" y 298 escaladas al fabricante.

OPERACIÓN SOC Y GESTIÓN DE EVENTOS DE SEGURIDAD

En lo referente al componente de monitoreo continuo, el SOC 7x24x365 operado por Growdata bajo el contrato, mantuvo operación ininterrumpida durante los siete períodos evaluados.

La infraestructura de monitoreo creció de 75 dispositivos integrados al FortiSIEM (diciembre 2025 – marzo 2026) a 77 (abril – junio 2026) y 78 (julio 2026), mediante métodos de recolección SNMP, Syslog y WMI.

A lo largo del período, se gestionaron y cerraron un total de 232 eventos de seguridad escalados al equipo perimetral, distribuidos de la siguiente manera: 69 en diciembre 2025 – enero 2026 (59 cerrados y 10 en seguimiento al corte del período), 56 en enero–febrero 2026 (todos cerrados), 28 en febrero–marzo 2026 (todos cerrados), 25 en marzo–abril 2026 (24 cerrados y 1 en seguimiento activo TK-1408), 27 en abril–mayo 2026 (todos cerrados), 15 en mayo–junio 2026 (todos cerrados), y 12 en junio–julio 2026 (todos cerrados).

En ninguno de los siete períodos se formalizaron incidentes de seguridad de la información, dado que la totalidad de los eventos correspondieron a alertas gestionadas, validadas con el cliente y tráfico

 Empresa Nacional Promotora del Desarrollo Territorial S.A.	INFORME DE SEGUIMIENTO Y EVALUACIÓN (Trabajos de informes, seguimientos de ley y/o cumplimiento)	CÓDIGO:	F-AU-10
		VERSIÓN:	04
		VIGENCIA:	2025-06-12
	AUDITORÍA INTERNA	CLASIFICACIÓN:	IP

bloqueado oportunamente por los controles perimetrales, sin afectación a la confidencialidad, integridad o disponibilidad de los activos de información de la Sociedad.

La plataforma de gestión de tickets migró de GLPI (períodos diciembre 2025 – febrero 2026) a ICREA V (a partir del período febrero–marzo 2026), lo que permitió mayor trazabilidad y visualización del estado de los casos escalados.

INTELIGENCIA DE AMENAZAS Y GESTIÓN DE SUPERFICIE DE ATAQUE EXTERNA (EASM)

El módulo FortiRecon EASM, integrado con el FortiSIEM, permitió la identificación de vulnerabilidades en activos expuestos a internet.

Durante el período mayo–junio de 2026 se detectaron 10 CVEs activos en el host indicado en el documento (HTTPS/4xx), con un recuento acumulado de 4.248 ocurrencias.

Adicionalmente, en el período junio–julio de 2026 (REC-001) se identificaron activos con alta concentración de puertos HTTP expuestos sin controles compensatorios suficientes (puerto indicado en el documento original de GTI) FortiRecon detectó también credenciales corporativas @enterritorio.gov.co en listas de combinación (combolists) filtradas, con acciones correctivas documentadas (TK-3890; REC-005, cuenta xxxx@enterritorio.gov.co deshabilitada – Ticket 6632/Caso 2844); sin embargo, el patrón recurrente de exposición orienta al análisis de fortalecimiento de la política de autenticación multifactor (MFA) para las cuentas institucionales.

Durante el período abril–mayo de 2026, el módulo EASM no reportó resultados de CVEs activos ("No report results found").

BOLETINES DE SEGURIDAD Y AMENAZAS RELEVANTES

De acuerdo a los documentos aportados, el contratista emitió boletines de seguridad mensuales sobre vulnerabilidades y amenazas emergentes.

Entre las más relevantes del período se destacan las siguientes:

- i) CVE-2025-59718 (autenticación FortiGate FortiCloud SSO bypass, FortiOS 7.4.9/7.4.10);
- ii) Campaña de correo malicioso suplantando notificaciones judiciales, con puntuación sandbox de 100/100 y técnica de evasión mediante extensión .svg; INCIBE-2026-124 (Nextcloud Talk <2026.2.2); CVE-2026-26980 (Ghost CMS, inyección SQL);
- iii) Actor de amenaza STORM-1175 operador del ransomware Medusa RaaS, con explotación de más de 16 CVEs incluyendo CVE-2026-23760 (CVSS 10.0, Crítico);
- iv) CVE-2026-34621 (Adobe Acrobat Reader – ejecución remota de código mediante PDF malicioso);
- v) CVE-2026-32201 (Microsoft SharePoint – spoofing sin autenticación);
- vi) CVE-2026-40976 (Spring Boot crítico, parche 4.0.6); y
- vii) CVE-2026-40372 (ASP.NET Core – escalamiento de privilegios a SYSTEM).

 Empresa Nacional Promotora del Desarrollo Territorial S.A.	INFORME DE SEGUIMIENTO Y EVALUACIÓN (Trabajos de informes, seguimientos de ley y/o cumplimiento)	CÓDIGO:	F-AU-10
		VERSIÓN:	04
		VIGENCIA:	2025-06-12
	AUDITORÍA INTERNA	CLASIFICACIÓN:	IP

El monitoreo activo del ecosistema de amenazas se soportó en fuentes de la comunidad FIRST (Emerging Threat, FortiGuard, Proofpoint, C2 Tracker, IPSum, entre otras) y en alertas preventivas institucionales, incluyendo un boletín específico para el contexto del período electoral (período febrero–marzo 2026).

CAPACIDADES TECNOLÓGICAS COMPLEMENTARIAS

De las evidencias documentales se identificó que, a partir del período junio–julio de 2026 se efectuó la incorporación de nuevas capacidades al ecosistema de seguridad tecnológica: FortiSandbox analizó 18.292 archivos durante el período, clasificando el 99,97% como limpios y sin detectar archivos maliciosos de severidad alta o media; FortiDeceptor OnPremise y Cloud fueron activados como tecnología para la detección de movimiento lateral y acceso no autorizado a activos señuelo.

Asimismo, FortiDLP (Protección de Datos) operó activamente desde el período mayo–junio de 2026, con 299 eventos DLP-USER detectados en el período junio–julio de 2026.

En este último período, se detectó actividad de correo con contenido malicioso originada desde la cuenta interna xxx@enterritorio.gov.co (7 y 8 de julio de 2026), sobre la cual el contratista emitió la recomendación REC-003.

- Resultado del análisis documental:

De los soportes documentales analizados, la Asesoría de Control Interno identificó que el contratista implementó un proceso estructurado de gestión y remediación de vulnerabilidades técnicas, soportado en herramientas especializadas (Nessus Professional, FortiRecon EASM, FortiSIEM, FortiSandbox, FortiDeceptor) y en la operación continua del SOC 7×24×365, con protocolo de gestión documental conforme al Procedimiento SIC-PR-03 y alineado con el Control 8.8 de la norma ISO/IEC 27001:2022.

No obstante, se identificaron en los soportes documentales que, las tasas de remediación del 3,6% en el entorno de Producción CCP y del 12,8% en Pruebas/CCA, lo cual indica que la mayoría de vulnerabilidades identificadas permanecen sin remediar al corte de la entrega de los soportes documentales.

En consecuencia, el criterio D01-2 se califica con **CUMPLIMIENTO PARCIAL**, reconociendo la existencia y operación del proceso de gestión de vulnerabilidades, pero considerando relevante la necesidad de fortalecer la ejecución de actividades de remediación y el seguimiento a los activos con mayor exposición en el entorno de producción y en la superficie de ataque externa.

- D01-3

Criterios: ISO/IEC 27001:2022

A.8.8 – Gestión de vulnerabilidades técnicas

A.8.29- Pruebas de seguridad en desarrollo y aceptación. Cubre las pruebas de seguridad sobre sistemas (incluye pruebas de intrusión sobre aplicaciones y entornos)

Criterio de verificación (Anexo Técnico No. 2):

	INFORME DE SEGUIMIENTO Y EVALUACIÓN (Trabajos de informes, seguimientos de ley y/o cumplimiento)	CÓDIGO:	F-AU-10
		VERSIÓN:	04
		VIGENCIA:	2025-06-12
	AUDITORÍA INTERNA	CLASIFICACIÓN:	IP

"El CONTRATISTA deberá suministrar, a través de un tercero certificado para ello, el servicio de pentesting (prueba de intrusión controlada) mínimo una (1) vez por año, durante el plazo de ejecución del contrato.

Los componentes a los que se le debe efectuar pentesting corresponden con los relacionados en los Anexos 1, 3, 4 y 5 (es decir, todos los componentes de la plataforma tecnológica).

El CONTRATISTA deberá presentar un informe con los resultados de las pruebas de pentesting, así como un Plan de Mejoramiento que contemple la solución o mitigación de las vulnerabilidades encontradas."

El 9 de septiembre de 2026, el GIT aportó 2 informes de pruebas de intrusión ejecutadas durante la vigencia 2026, ambos elaborados y revisados por un profesional en calidad de responsable técnico.

1) Informe de Pentesting Caja Gris (PT-D01-3-E1):

El documento denominado "Informe de Pentesting Caja Gris — ENTerritorio", versión 1.0, con fecha del 12 de junio de 2026, fue ejecutado bajo la modalidad de caja gris con acceso limitado, sin conectividad a la LAN/WLAN corporativa interna (condición reconocida en el documento como limitación metodológica).

El alcance comprendió las redes inalámbricas visibles en el perímetro evaluado, dispositivos inalámbricos no reconocidos y controles de segmentación, excluyendo expresamente: Directorio Activo, LDAP, Kerberos, SMB/RPC, bases de datos, servidores internos, movimiento lateral y pruebas de explotación intrusiva o destructiva. La metodología siguió las fases: Planeación y alcance / Reconocimiento inalámbrico / Validación de alcance / Análisis de riesgo / Recomendaciones.

En la sección de resultados, se identificaron 4 hallazgos en reconocimiento inalámbrico:

- i) WIFI-01 — Redes o dispositivos inalámbricos no reconocidos visibles (riesgo Medio),
- ii) WIFI-02 — Exposición de nombres de dispositivos móviles o metadatos identificables (riesgo Medio),
- iii) WIFI-03 — Redes configuradas como ocultas visibles mediante tráfico de administración (riesgo Bajo/Medio), y
- iv) WIFI-04 — Capacidades BLE/Zigbee observables en puntos de acceso o dispositivos cercanos (riesgo Medio).

La validación de activos internos críticos, confirmó que no se obtuvo acceso efectivo al Directorio Activo, bases de datos, servidores internos ni repositorios corporativos; el análisis de exfiltración, determinó que no se identificó ruta técnica viable y que la cadena de ataque no se materializó durante el ejercicio.

Las conclusiones indicadas en los soportes documentales, señalan que la superficie de ataque presentó un nivel de exposición controlado, sin evidencia de compromisos a la confidencialidad, integridad o disponibilidad de la información bajo las condiciones evaluadas, y que los controles de segmentación, restricción de acceso y protección perimetral resultaron efectivos. El informe propone como actividad complementaria, la ejecución de un ejercicio de mayor profundidad sobre componentes internos con alcance y autorizaciones formales previamente definidas.

 Empresa Nacional Promotora del Desarrollo Territorial S.A.	INFORME DE SEGUIMIENTO Y EVALUACIÓN (Trabajos de informes, seguimientos de ley y/o cumplimiento)	CÓDIGO:	F-AU-10
		VERSIÓN:	04
		VIGENCIA:	2025-06-12
	AUDITORÍA INTERNA	CLASIFICACIÓN:	IP

2) Informe de Pentesting Web Caja Negra (PT-D01-3-E2)

El documento denominado "Informe de Pentesting Web — ENTerritorio", versión 1.0, con fecha del 20 de abril de 2026 y fecha de creación del documento del 20 de marzo de 2026, fue ejecutado bajo la modalidad de caja negra (black box) con base en el marco OWASP Top 10:2025.

Las herramientas utilizadas fueron: Nessus (escaneo activo de vulnerabilidades), BurpSuite (análisis de tráfico y pruebas de inyección), Amass y Subfinder (enumeración pasiva de subdominios) y ZoomEye (reconocimiento OSINT/geolocalización). Los hallazgos se clasificaron bajo el estándar CVE/CWE.

El alcance cubrió 18 URLs del dominio enterritorio.gov.co, de las cuales 4 resultaron accesibles durante la prueba (enterritorio.gov.co, elearning.enterritorio.gov.co, lira.enterritorio.gov.co y sgp.enterritorio.gov.co), 4 con acceso restringido (pilotosiscoadmin, siscosradmin, siscosusuarios y pilotosiscoformularios) y 10 sin resolución DNS activa.

La infraestructura identificada incluyó servicios alojados en AWS, IFX Networks Colombia.

El escaneo activo mediante Nessus arrojó un total de 547 vulnerabilidades, distribuidas así: 7 críticas (5 en seconef.enterritorio.gov.co, 1 en entowncloud.enterritorio.gov.co y 1 en sso.enterritorio.gov.co); 16 altas (6 en seconef, 8 en portalsigep.enterritorio.gov.co y 2 en entowncloud); 44 medias; 22 bajas; y 458 informativas. El detalle completo de hallazgos reposa en los anexos "Matriz_Hallazgos-Web_Enterritorio.xlsx" y "Reportes Burp Suite 2026", aportados como parte del informe. El análisis bajo el Marco OWASP Top 10:2025, evaluó las 10 categorías de riesgo.

- Resultado de la verificación documental:

Con base en el análisis de los soportes documentales aportados, este control se valora como **CUMPLE**.

Se identificaron 2 ejercicios de prueba de intrusión controlada durante la vigencia 2026, realizados por un profesional, bajo metodologías reconocidas internacionalmente (caja gris y caja negra/OWASP Top 10:2025), con cobertura sobre el entorno inalámbrico perimetral y el entorno web institucional.

Los informes presentan estructura con identificación de hallazgos con clasificación de riesgo, recomendaciones priorizadas y conclusiones sobre el nivel de exposición.

En los soportes documentales, se dejó constancia de que la prueba de caja gris fue ejecutada con acceso limitado y sin conectividad a los activos internos de mayor criticidad, condición reconocida en el informe como limitación metodológica y que motiva la propuesta de una fase complementaria.

D01-4

Criterios: ISO/IEC 27001:2022

A.8.19 – Instalación de software en sistemas operativos

A.8.8 Gestión de vulnerabilidades técnicas Complementario

A.8.32 – Gestión de cambios

	INFORME DE SEGUIMIENTO Y EVALUACIÓN (Trabajos de informes, seguimientos de ley y/o cumplimiento)	CÓDIGO:	F-AU-10
		VERSIÓN:	04
		VIGENCIA:	2025-06-12
	AUDITORÍA INTERNA	CLASIFICACIÓN:	IP

Criterio de verificación (Anexo Técnico No. 2):

*“ACTUALIZACIÓN: Se requiere que el **Contratista actualice y mantenga los sistemas operativos** de los servidores, estaciones de trabajo y equipos que lo requieran. Este procedimiento se debe ejecutar al menos 3 veces al año o cuando los fabricantes publiquen actualizaciones críticas de seguridad.*

El plan de actualización debe ser presentado al supervisor del contrato y aprobado por este al inicio de cada vigencia. //

Deberá ejecutarse gradualmente de forma que se mantenga la compatibilidad y funcionalidad de los sistemas existentes. //

Deberá contemplarse mecanismos para regresar (Rollback) a la versión anterior de forma que si las actualizaciones fallan se pueda revertir el procedimiento realizado y continuar con la operación normal.”

El 17 de septiembre de 2026, el GTI remitió 16 soportes documentales, codificados PT-D01-4-E1 a PT-D01-4-E16.

Los primeros cuatro ,corresponden a capturas de pantalla del entorno tecnológico: PT-D01-4-E1 es la consola FortiEDR (fortixdrconnectlat3.console.ensilo.com), que muestra 254 de 500 licencias activas, 123 colectores inactivos y la funcionalidad eXtended Detection sin licenciar; PT-D01-4-E2 corresponde a la configuración del módulo File Scan de FortiEDR, con escaneo semanal los domingos a las 02:00 AM y último escaneo ejecutado el 13-Sep-2026; PT-D01-4-E3 es la captura del módulo "Update Collector Version" de FortiEDR, que muestra la versión instalada 6.1.1 Rev.1292 y la versión disponible 6.2.0 Rev.1437 sin aplicar; PT-D01-4-E4 corresponde a la consola de Administración de Directivas de Grupo (GPO "Update_Equipos") aplicada sobre la OU "Estaciones Fonade" en el dominio fonade.net, servidor AD 172.16.1.60. Las evidencias PT-D01-4-E5 a PT-D01-4-E15 corresponden a 11 Informes Mensuales de Monitoreo SOC elaborados por GrowData, cubriendo el período agosto 2025 a julio 2026, aportados por GTI como evidencias de referencia del ítem III.2 de la solicitud de información, para sustentar las actualizaciones de servidores. Finalmente, PT-D01-4-E16 corresponde a la respuesta escrita del GTI al criterio D01-4.

- Análisis por eje de criterio:

i). Actualizaciones de servidores. GTI refirió los Informes SOC mensuales (soportes documentales del ítem III.2) como sustento de las actualizaciones de servidores. Sin embargo, estos informes documentan la operación del servicio de monitoreo de seguridad con FortiSIEM (incluyendo gestión de eventos, dispositivos integrados, inteligencia de amenazas y recomendaciones de seguridad) pero no contienen registros de parches de SO aplicados, inventario de versiones actualizadas por servidor, ni cronograma de actualizaciones ejecutado. La referencia a los informes SOC como evidencia de patching de servidores es insuficiente para acreditar el cumplimiento de este requerimiento.

ii) Actualizaciones de estaciones de trabajo. Se acredita la existencia de la GPO "Update_Equipos" sobre la OU "Estaciones Fonade" en el dominio fonade.net como mecanismo de despliegue de actualizaciones en estaciones. GTI mencionó adicionalmente la existencia de un servidor WSUS para

	INFORME DE SEGUIMIENTO Y EVALUACIÓN (Trabajos de informes, seguimientos de ley y/o cumplimiento)	CÓDIGO:	F-AU-10
		VERSIÓN:	04
		VIGENCIA:	2025-06-12
	AUDITORÍA INTERNA	CLASIFICACIÓN:	IP

actualización automática de SO. No obstante, no se aportó captura de la consola WSUS que permita verificar el inventario de equipos registrados, los parches aprobados y desplegados, ni el estado de cumplimiento por máquina. La GPO evidencia el mecanismo de distribución pero no el estado real de actualización del parque de estaciones.

iii). Plan formal de actualización. No se aportó documento de plan de actualización presentado al supervisor del contrato y aprobado por este al inicio de la vigencia. Este es un requisito del criterio objeto de análisis, cuyo incumplimiento implica que la ejecución de actualizaciones carece de marco de referencia, trazabilidad y supervisión contractual.

iv). Rollback y mitigación de incompatibilidades. No se evidencian procedimientos documentados de rollback ante fallas en actualizaciones de SO, ni protocolos de mitigación ante incompatibilidades SO/firmware/equipo. Ambos son requerimientos del criterio.

- **Resultado de la verificación documental:**

Los componentes analizados fueron evidenciados a través de soportes documentales, estos son: La existencia de un mecanismo GPO para estaciones de trabajo y la operación continua del servicio SOC/FortiSIEM con 13 informes mensuales consecutivos.

De otro lado, no fueron evidenciados en los soportes documentales, el plan formal de actualización aprobado por el supervisor, y los mecanismos formales de rollback y mitigación de incompatibilidades.

Dado lo anterior, este criterio se identificó con **CUMPLIMIENTO PARCIAL**.

- **D.01-5:**

Criterios: ISO/IEC 27001:2022

A.5.37 – Documentación de procedimientos

A.8.9 – Config. Segura

Criterio de verificación (Anexo Técnico No. 2):

“HARDENING: Evaluación del estado real de seguridad de un dispositivo.

El Contratista debe realizar el hardening previo a la entrada en producción de los siguientes componentes [en CCP, CCA, CCB y ACH]: Sistemas operativos, Virtualizadores, Bases de datos, Software y servidores de aplicaciones, Sistemas en nube pública, Sistemas de enrutamiento y conmutación, Circuito Cerrado de Seguridad. //

DESCRIPCIÓN INFRAESTRUCTURA: Centro de Datos Principal CCP, Centro de Datos Alterno CCA, Centro de Comunicaciones Básico CCB (calle 26 No 13-19), Sede Archivo Central Histórico ACH (calle 12 No. 79a-25)."

El GTI el 17 de septiembre de 2026, aportó los siguientes soportes documentales e indicó lo siguiente en la respuesta: “Nos apoyamos inicialmente en las evidencias de la respuesta D01-1 y adicionalmente

 Empresa Nacional Promotora del Desarrollo Territorial S.A.	INFORME DE SEGUIMIENTO Y EVALUACIÓN (Trabajos de informes, seguimientos de ley y/o cumplimiento)	CÓDIGO:	F-AU-10
		VERSIÓN:	04
		VIGENCIA:	2025-06-12
	AUDITORÍA INTERNA	CLASIFICACIÓN:	IP

presentamos evidencia de la plataforma de monitoreo de los componentes y servicios en cada uno de los data centers Zabbix, donde se monitorea y gestiona cuando se presenta alguna incidencia o se requiere cambio de hardware”.

Actas Internas de Seguimiento:

- Acta 03/2026** (05-Feb-2026): Hardening firmware FortiGate en 4 sedes — CCP 7.4.9→7.4.11 (Cambio 2342), CCA 7.4.10→7.4.11 (Cambio 2340), ACH 7.4.10→7.4.11 (Cambio 2343), CCB 7.4.6→7.4.11 (Cambio 2344), CCB FSSO 5.0.0.314→5.0.0330 (Cambio 2341). CSP hardening Apache/Drupal (Cambio 2331). Restricción acceso FortiGate/FortiPAM (A44). Rollback KVM CCA (Cambio 2336).
- Acta 12/2026** (16-Apr-2026): FortiSIEM upgrade 7.2→7.5 (Cambio 2367, servidor CCP listo, colector pendiente). ROI security fixes JS (cambio pendiente).
- Acta 13/2026** (23-Apr-2026): FortiSIEM collector laaS actualizado. ROI WAF integration (Cambio 2390). ERP security fixes (Cambios 2391–2393). IPv6 (Cambio 2394).
- Acta 14/2026** (30-Apr-2026): Azure security score 88% (Cambio 2387). WAF enthubincumplimientos y enthubproyectos (Cambio 2396).

Reportes ZAP by Checkmarx v2.17.0 (4 PDFs):

- 2026-01** (16-Ene-2026): roi.enterritorio.gov.co — 2 Alto (SQLi Time-Based x2, Redirección Externa x14), 5 Medio (Anti-CSRF, CSP issues)
- 2026-02** (12-Mar-2026): OPE_INUSUALES — 2 Alto (Librería JS Vulnerable, Redirección Externa x15), 4 Medio
- 2026-03** (20-Mar-2026): OPE_INUSUALES — 1 Alto (Redirección Externa x30), 4 Medio (nuevos hallazgos: .env leak, Directory Browsing)
- 2026-04** (27-Mar-2026): OPE_INUSUALES Azure+172.16.7.41 — **0 Alto, 2 Medio** → remediación verificada

Correos electrónicos - ciclo ZAP (6 MSG):

- VALIDA1.MSG** (27-Feb-2026): profesional xxxx a xxxx — Aclaración técnica de falsos positivos de SQLi del scan de enero (URLs afectadas son archivos estáticos CSS/JS sin consultas a BD)
- RE_ROI1.MSG**: Solicitud y resultados de escaneo roi.enterritorio.gov.co
- RE_SOL1.MSG**: Solicitud escaneo OPE_INUSUALES; GTI realizó análisis desde VPN C2S hacia http://172.16.x.xx/OPE_INUSUALES/
- INFORM1.MSG** (31-Mar-2026): Informe análisis ZAP para OPE_INUSUALES (fecha 31-Mar-2026), presenta resultados de severidad
- RE_INF1.MSG**: Seguimiento con creación de Caso No. 2384 / CHG-143050-9-2384 para remediación
- RE_RES1.MSG**: Confirmación de remediación: "ya no se presenta vulnerabilidades de nivel crítico o alto, la de nivel medio que aparecen son 2. La ausencia de token anti-CSRF es un falso positivo (...) el formulario si tiene el token aplicado y funcional."

 Empresa Nacional Promotora del Desarrollo Territorial S.A.	INFORME DE SEGUIMIENTO Y EVALUACIÓN (Trabajos de informes, seguimientos de ley y/o cumplimiento)	CÓDIGO:	F-AU-10
		VERSIÓN:	04
		VIGENCIA:	2025-06-12
	AUDITORÍA INTERNA	CLASIFICACIÓN:	IP

Reportes de Disponibilidad Zabbix 7.4.2 (6 PDFs):

Reporte	Período	Hosts	Disponibilidad	CUMPLE	REGULAR	CRÍTICO
DISPON1/2	27-Mar → 26-Abr-2026	167	99.94%	166	1	0
DISPON3	27-Abr → 26-May-2026	115	99.84%	111	4	0
DISPON4	27-May → 26-Jun-2026	115	99.55%	111	3	1*
DI68A41	27-Jun → 26-Jul-2026	116	99.94%	115	1	0
DI6C981	27-Jul → 26-Ago-2026	117	99.61%	105	9	3**

*DISPON4 CRÍTICO: ENTSRVSGDEACOMPODES (63.95%) — CCP PRUEBAS (entorno no productivo)

**DI6C981 CRÍTICO: ENTSRVNESSUS (92.74%), ENTSRVREPONESSUS (94.60%), FONSRVSISCOMPRU (89.08%) — escáner de vulnerabilidades Nessus y componente Cisco en entorno de pruebas

Grupos monitoreados en Zabbix: Applications, CCA, CCB Calle 26, CCP Producción, CCP Pruebas, Firewalls ENTerritorio (FW-ACH, FW-CCA, FW-CCB, FW-CCP), KVM (hypervisors), Networking (switches SW-xx-Fortinet-448E, SW-CORE-Fortinet-1048E), Zabbix Servers.

Evidencias cambios en ARANDA (2 DOCX — solo capturas de pantalla, no legibles en texto):

- i. Evidencias_Cambios_Parchado.docx: Registros Cambios 2096, 2120, 2123, 2170, 2199, 2218, 2200, 2228, 2250, 2295, 2348, 2360, 2387, 2407, 2403, 2418, 2430, 2459, 2470
- ii. Evidencias_Cambios_en_Aranda.docx: Registros Cambios 2191, 2232, 2281, 2306, 2314, 2324, 2344, 2357, 2388, 2389, 2425, 2444, 2445, 2454, 2465, 2466, 2467, 2471, 2478

- Análisis por eje de criterio:

1. Sistemas Operativos

Los soportes documentales cubren la actualización del SO de appliances de seguridad (FortiGate firmware upgrades en las 4 sedes, registrados como Cambios ARANDA). Los servidores CCP, CCA, CCB aparecen monitoreados en Zabbix. Sin embargo, no se aportó evidencia de hardening del SO de servidores de propósito general (benchmarks CIS, DISA STIG, o procedimiento equivalente).

2. Virtualizadores

KVM monitorizado en Zabbix (ENTLUMOLKVM, KVM-STORAGE, entccpkvm01/02.fonade.net). Acta 03/2026 registra rollback de KVM CCA (gestión activa). No se aportó evidencia de hardening de hipervisores (deshabilitación servicios no requeridos, restricción de acceso a consola, cifrado de comunicaciones).

3. Bases de Datos

ENTSRVSQL01/02 y ENTSRVSGDEAMONGO monitorizados en Zabbix. No se aportó soporte documental de hardening de motores de base de datos (Oracle, SQL Server, MongoDB).

4. Software y Servidores de Aplicaciones

Es el componente presenta los siguientes soportes documentales: hardening CSP en Apache/Drupal

 Empresa Nacional Promotora del Desarrollo Territorial S.A.	INFORME DE SEGUIMIENTO Y EVALUACIÓN (Trabajos de informes, seguimientos de ley y/o cumplimiento)	CÓDIGO:	F-AU-10
		VERSIÓN:	04
		VIGENCIA:	2025-06-12
	AUDITORÍA INTERNA	CLASIFICACIÓN:	IP

(Cambio 2331), escaneos ZAP con ciclo completo documentado para ROI y OPE_INUSUALES (solicitud → escaneo → informe → cambio ARANDA → remediación → validación → cierre), ERP security fixes (Cambios 2391–2393), Apache Tomcat en producción (visible en SIEMCOLLEC).

5. Sistemas en Nube Pública

Azure security score 88% documentado (Cambio 2387, Acta 14/2026). WAF implementado para 3 aplicaciones en Azure (Cambio 2390, 2396). IPv6 publicación normativa (Cambio 2394). Limitación: el 12% restante sin documentación de plan de mejora ni detalle de hallazgos pendientes en Azure Security Center.

6. Sistemas de Enrutamiento y Conmutación

FortiGate en las 4 sedes con firmware actualizado a 7.4.11 y restricciones de acceso (FortiGate/FortiPAM, A44). Switches Fortinet (448E y 1048E) monitoreados en Zabbix. FortiSIEM actualizado 7.2→7.5. Sin embargo, no hay evidencia de hardening formal de switches (VLAN hardening, protocolos de gestión seguros, deshabilitación de puertos no utilizados, SNMP v3).

7. Circuito Cerrado de Seguridad (CCTV)

Ninguno de los 22 soportes documentales hace referencia al sistema CCTV. No hay mención en las actas, Zabbix, ni correos electrónicos.

- Resultado de la verificación documental:

Los soportes documentales permiten identificar un proceso activo de seguridad tecnológica con gestión de cambios (ARANDA/ITIL), monitoreo continuo integral (Zabbix), escaneos de vulnerabilidades (ZAP by Checkmarx) con ciclo completo de remediación para aplicaciones web, y actualizaciones de firmware de seguridad en las 4 sedes. Sin embargo, la documentación es insuficiente para verificar hardening previo a producción de: i) SO de servidores de propósito general, ii) bases de datos, iii) virtualizadores bajo benchmarks reconocidos, iv) switches de conmutación, y v) del CCTV no se aportaron soportes documentales.

Dado lo anterior, se establece **CUMPLIMIENTO PARCIAL** del criterio.

- **D01-6**

Criterios: ISO/IEC 27001:2022

A.8.8 – Gestión de vulnerabilidades técnicas

Criterio de verificación (Anexo Técnico No. 2):

“GESTIÓN DE VULNERABILIDADES: El CONTRATISTA deberá **presentar un informe con los resultados de las pruebas de pentesting** (prueba de intrusión controlada), así como un **Plan de Mejoramiento que contemple la solución o mitigación de las vulnerabilidades encontradas.** //

Como valor de referencia en la actualidad se presenta un promedio de 400 vulnerabilidades por año.”

	INFORME DE SEGUIMIENTO Y EVALUACIÓN (Trabajos de informes, seguimientos de ley y/o cumplimiento)	CÓDIGO:	F-AU-10
		VERSIÓN:	04
		VIGENCIA:	2025-06-12
	AUDITORÍA INTERNA	CLASIFICACIÓN:	IP

- **Análisis por eje de criterio:**

i). Informe de pruebas de pentesting / detección de vulnerabilidades:

En los soportes documentales, se evidenció la existencia de infraestructura Nessus (servidor ENTSRVREPONESSUS documentado en Caso 2351, Feb-2026) de lo cual, el GTI mencionó explícitamente el "informe Nessus" como entrega en la matriz adjunta a la respuesta. Sin embargo, no se identificó en los soportes documentales el documento indicado.

Los reportes de detección de vulnerabilidades corresponden a los escaneos ZAP by Checkmarx v2.17.0 de sesiones anteriores (ROI y OPE_INUSUALES).

En este sentido, la acreditación del informe de pentesting (conforme al criterio del Anexo No. 2) no fue verificado por ausencia de soporte documental.

ii). Plan de Mejoramiento formal:

No se evidenció un documento consolidado de Plan de Mejoramiento. En los soportes documentales se identificó el ciclo operativo de gestión: vulnerabilidades detectadas → RFC aprobado en comité → ejecución con ventana de cambio → evidencia técnica de ejecución → cierre de caso Aranda.

Como ya se indicó, el requisito central del criterio (presentar el informe formal de pentesting) no quedó evidenciado, y por consecuencia la claridad específica frente a, si fue necesario que se aportara un Plan de Mejoramiento consolidado como entregable, no se identificó.

iii). Ejecución del programa de remediación:

Los soportes documentales identificaron un programa activo y sostenido de remediación con dos componentes:

i) Parchado de servidores: 25 casos Aranda documentados a lo largo del período, cubriendo servidores Oracle Linux 8/9, Red Hat 8, Windows y Oracle DB en CCP, CCA y entornos de prueba. Las frecuencias de actualización son trimestral/mensual (servidor ENTSRVBANC muestra actualizaciones en: nov-2025 [105 paquetes], ago-2025 [82], jun-2025 [99], mar-2025 [107], nov-2024 [119]). El proceso incluye toma previa de snapshots para rollback, evidenciada con cierre de casos NetSuite.

ii) Actualización de firmware FortiGate: 13 eventos documentados en las 4 sedes (CCP, CCA, CCB, ACH) entre ago-2025 y jun-2026, cubriendo versiones 7.4.7 → 7.4.8 → 7.4.9 → 7.4.11 → 7.4.12. Cada actualización tramitada vía RFC y caso Aranda.

- **Resultado de la verificación documental:**

A través de los soportes documentales, se identificó un programa operativo de gestión de vulnerabilidades con actividad sostenida (parchado mensual de servidores, actualización trimestral de firmware de firewalls, control de cambios vía Aranda).

 Empresa Nacional Promotora del Desarrollo Territorial S.A.	INFORME DE SEGUIMIENTO Y EVALUACIÓN (Trabajos de informes, seguimientos de ley y/o cumplimiento)	CÓDIGO:	F-AU-10
		VERSIÓN:	04
		VIGENCIA:	2025-06-12
	AUDITORÍA INTERNA	CLASIFICACIÓN:	IP

No obstante, el requisito central del criterio (presentar el informe formal de pentesting) no quedó evidenciado, y por consecuencia la claridad específica frente a si fue necesario que se aportara un Plan de Mejoramiento consolidado como entregable, no se identificó.

Dado lo anterior, se especificó el **CUMPLIMIENTO PARCIAL** del criterio objeto de evaluación.

- **Dominio D04:**

Tabla 3 Obligaciones principales del Dominio 04

N.º	Componente / Dimensión	Descripción y Obligaciones Principales	Norma / Marco Aplicable
5	D04 – SOC / SIEM / Monitoreo / Análisis Forense	SOC 7x24x365 con personal calificado SIEM: mínimo 1.000 EPS o 100 dispositivos monitoreados Correlación de eventos e inteligencia de amenazas Retención de logs: mínimo 6 meses Análisis forense digital: mínimo 2 análisis/año Gestión y respuesta a incidentes de seguridad	ISO 27001:2022, Anexo A: A.8.15 – Registro de eventos (logging) A.8.16 – Actividades de monitoreo ISO/IEC 27035:2023 – Gestión de incidentes de SI ISO/IEC 27037:2012 – Evidencias digitales NOGAI 2024 – Principios 13 a 15

- **D04-1**

ISO/IEC 27001:2022

A.8.15 – Registro de eventos

A.8.16 – Monitoreo de actividades

Criterio de verificación (Anexo Técnico No. 2, Numeral 4):

"El contratista deberá prestar los servicios de ciberseguridad, SOC (Centro de Operaciones de Seguridad), para ello deberá realizar seguimiento y análisis de la actividad de la red, servidores, puntos finales, bases de datos, aplicaciones y sitios web, en horario 7x24x365, buscando eventos anómalos que puedan ser indicio de un incidente o compromiso de seguridad. Mejorando la capacidad de vigilancia, detección y respuesta a amenazas en la operación diaria de la Entidad.

*El contratista deberá validar que los **posibles eventos e incidentes de seguridad** se identifiquen, analicen, defiendan, investiguen e informen correctamente, cumpliendo con los parámetros, las mejores prácticas en seguridad, y normatividad establecida en la Entidad, para ello como mínimo debe cumplir:*

Monitoreo centralizado de logs y correlación de eventos: Contar con las herramientas para correlacionar eventos y logs en tiempo real. El sistema SIEM recopilará los eventos de todos los dispositivos de red, seguridad, autenticación (Directorio Activo), servidores bases de datos, aplicaciones, sitios web, que el supervisor del contrato determine."

 Empresa Nacional Promotora del Desarrollo Territorial S.A.	INFORME DE SEGUIMIENTO Y EVALUACIÓN (Trabajos de informes, seguimientos de ley y/o cumplimiento)	CÓDIGO:	F-AU-10
		VERSIÓN:	04
		VIGENCIA:	2025-06-12
	AUDITORÍA INTERNA	CLASIFICACIÓN:	IP

Como soportes documentales del cumplimiento de este criterio, el GTI aportó el reporte denominado "Reporte Fuentes Integradas en el FortiSIEM — Approved Devices" (PT-D04-1-E1), generado desde la plataforma FortiSIEM el día 07 de septiembre de 2026 a las 09:38:05 a.m.

El reporte evidenció un total de 78 dispositivos aprobados e integrados activamente en la plataforma de correlación y monitoreo centralizado de eventos, con identificación de nombre de dispositivo, dirección IP, fabricante, modelo de tipo de dispositivo y fecha de descubrimiento/integración.

El análisis de las fuentes integradas confirmó la siguiente cobertura por categoría de activo tecnológico, en concordancia con el alcance requerido por el Anexo Técnico No. 2:

- Análisis por eje de criterio:

i) Dispositivos de red y seguridad perimetral: Se verificó la integración de los firewalls FortiOS de los 4 nodos de infraestructura: FW_MAIN_CCP (172.16.xxx.xxx), FW_MAIN_CCA (172.16.xxx.xxx), FW_MAIN_CCB (172.16.xxx.x) y FW_MAIN_ACH (172.xxx xxx.1), así como los firewalls del entorno Azure FWFORTIGATE-fgt (172.17.x.x) y FWBfortigate-fgt (172.xx.x.xx). Se identificaron igualmente dos (2) switches de núcleo de la marca Fortinet modelo 1048E (SW-CORE-1 en 192.168.xxx.x y SW-CORE-2 en 192.168.xxx.x) y un FortiSwitch adicional (S448EFTF23022486 en 10.xxx.x.2).

ii) Servidores Windows (Microsoft): Se confirmó la integración de 19 servidores Windows con sistemas operativos Windows Server 2012 R2, 2016, 2019 y 2022, correspondientes a funciones de respaldo (FONSRVRESPALDO, FONSRVRESPALDO1), base de datos (ENTSRVSQL01 — 172.16.x.xxx, ENTSRVSQL02 — 172.16.x.xxx), sincronización de directorios (ENTSRVDSYNC), DHCP (FONSRVDHCP01, FONSRVDHCP3), aplicaciones de negocio (FONSRVNIIF, FONSRVHELISA, FONSRVHELISA02, FONSRVSEVINPRO, FONSRVPOWERBI3) y autenticación RADIUS (ENTSRVRADIUS — 172.16.x.xx).

iii) Autenticación — Directorio Activo: Se verificó la integración de 4 controladores de dominio del entorno fonade.net: ENTSRVDC01 (172.16.x.xxx — Windows Server 2022), FONSRVDC03 (172.16.x.xx — Windows Server 2019), ENTLUMDC01 (172.16.x.xxx — Windows Server 2019) y FONSRVBDC04 (172.16.x.xx — Windows Server 2019), así como FONSRVAD04 (172.16.x.xxx — Windows Server 2016), cubriendo la fuente de autenticación centralizada conforme al requisito contractual de inclusión del Directorio Activo en el SIEM.

iv) Servidores Linux/Unix: Se identificaron 32 fuentes del tipo Linux/Unix, entre las cuales se encuentran múltiples instancias con prefijo IFX_NETWORKS (RedHat Linux), servidores de aplicación con prefijo ENTS y FONS en sistemas CentOS, RedHat y Unix genérico, incluyendo el servidor ENTSRVNTPLINUX (172.16.x.xx — RedHat) para sincronización de tiempo y el servidor ENTSRVAPACHE02 (172.16.x.x) para servicios web.

v) Soluciones de seguridad Fortinet integradas como fuentes: Adicionalmente al motor FortiSIEM (fortisient — 172.18.xx.x) y su nodo collector (collectorent — 172.16.x.xx), se evidenció la integración de: FortiDLP (us-1.fortidlp.forticloud.com — 34.111.xxx.xxx, integrado el 04 de mayo de 2026), FortiWeb Cloud (syslog.fortiappsec-cloud.com — 10.254.xx.x, integrado el 04 de mayo de 2026), FortiPAM (FORTIPAM — 20.109.xx.xx), FortiSandbox (172.16.x.xx, integrado el 06 de agosto de 2026) y FortiRecon (api.fortirecon.forticloud.com — 34.201.xx.xxx, integrado el 13 de enero de 2026).

 Empresa Nacional Promotora del Desarrollo Territorial S.A.	INFORME DE SEGUIMIENTO Y EVALUACIÓN (Trabajos de informes, seguimientos de ley y/o cumplimiento)	CÓDIGO:	F-AU-10
		VERSIÓN:	04
		VIGENCIA:	2025-06-12
	AUDITORÍA INTERNA	CLASIFICACIÓN:	IP

vi) Servicios en nube: Se confirmó la integración de Microsoft Office 365 (manage.office.com — 13.107.xxx.xx) como fuente de eventos en nube, en concordancia con el entorno Azure declarado en el Anexo Técnico No. 2.

- **Resultado de la verificación:**

Con base en el análisis de los soportes documentales, el criterio D04-1, se valora como **CUMPLE**.

El reporte de dispositivos aprobados generado directamente desde la consola de FortiSIEM el 07 de septiembre de 2026 acredita la integración activa de 78 fuentes de eventos, con cobertura comprobada sobre dispositivos de red (firewalls de los cuatro nodos de infraestructura CCP, CCA, CCB y ACH, así como entorno Azure), servidores Windows y Linux, controladores de dominio y autenticación RADIUS, bases de datos SQL, aplicaciones web (FortiWeb Cloud), servicios en nube (Office 365) y soluciones de seguridad especializadas (FortiDLP, FortiSandbox, FortiPAM, FortiRecon). Esta cobertura es consistente con el alcance requerido en el numeral 4 del Anexo Técnico No. 2 para el monitoreo centralizado en tiempo real 7x24x365.

La operación continua del SOC será verificada en el criterio D04-2.

- **D04-2**

Criterios: ISO/IEC 27001:2022

C.8.15 – Registro de eventos

C.8.16 – Monitoreo de actividades

Criterio de verificación (Anexo Técnico No. 2, Numeral 4):

*"El contratista deberá **validar que los posibles eventos e incidentes de seguridad se identifiquen, analicen, defiendan, investiguen e informen correctamente**, cumpliendo con los parámetros, las mejores prácticas en seguridad, y normatividad establecida en la Entidad, para ello como mínimo debe cumplir: [...]*

*Deberá tener la capacidad de realizar: **Detección en tiempo real de amenazas y actividades anómalas. Correlación de eventos e incidentes de diferentes dispositivos**, incluyendo plataformas de seguridad, servidores, switches, routers de diferentes fabricantes.*

***Posibilidad de generación de reglas de parsing para logs de eventos de plataformas que no estén soportadas. Personalización y parametrización de reglas de correlación.** Capacidad de procesamiento mínimo 1000 EPS o 100 dispositivos. Manejo de indicadores de compromiso. Integración con fuentes de inteligencia de amenazas de terceros. Alertas para prevención y detección de intrusiones y vulnerabilidades. Alertas de robo de información confidencial. Detectar, analizar, contener y remediar eventos e incidentes de seguridad que se puedan presentar. Detección de modificación de archivos o carpetas en servidores críticos. Detección de cambios de registro en servidores Windows. Deberá crear las alarmas de acuerdo con los niveles de criticidad que sean acordados con el supervisor del contrato."*

	INFORME DE SEGUIMIENTO Y EVALUACIÓN (Trabajos de informes, seguimientos de ley y/o cumplimiento)	CÓDIGO:	F-AU-10
		VERSIÓN:	04
		VIGENCIA:	2025-06-12
	AUDITORÍA INTERNA	CLASIFICACIÓN:	IP

Como soportes documentales de gestión del cumplimiento de este criterio, el GTI aportó el reporte denominado "Active Rules_SOC — Reporte de Reglas Activas" (PT-D04-2-E1), generado directamente desde la plataforma FortiSIEM el día 07 de septiembre de 2026 a las 09:39:47 a.m., correspondiente a la organización Super. El reporte evidencia un total de 123 reglas de correlación activas, parametrizadas y personalizadas para el entorno tecnológico de ENTerritorio S.A, distribuidas en 2 categorías operacionales:

i). Reglas NOC — 16 reglas activas (monitoreo de disponibilidad e infraestructura): Cubren la supervisión continua de los recursos de infraestructura, incluyendo alertas por latencia en disco, consumo crítico de memoria y CPU, aumento en tiempos de respuesta SNMP y WMI, caída de dispositivos ENTerritorio S.A, caída de interfaces del switch core, caída o intermitencia de páginas web (5 min), servicios automáticos detenidos, servidores sin respuesta de ping, ausencia de logs de dispositivos y problemas de operación de portales web. Estas reglas soportan directamente el monitoreo 7×24×365 del entorno requerido por el Anexo Técnico No. 2.

ii) Reglas SOC — 107 reglas activas (detección, correlación y alertas de seguridad): Abarcan las siguientes categorías de detección, correspondientes a las capacidades exigidas en el numeral 4 del Anexo Técnico No. 2:

- En control de acceso y autenticación, se verificaron reglas para detección de aumentos repentinos en inicios de sesión exitosos, autenticaciones VPN simultáneas desde diferentes países, cambios repentinos de ubicación de usuario, cuentas bloqueadas en dominio, errores de inicio de sesión de VPN desde fuera del país, múltiples fallos de inicio de sesión en dominio y VPN, inicio de sesión RDP y SMB remotos desde IP pública, sesiones VPN de larga duración, e inicios de sesión inusuales en Office 365.
- En detección de intrusiones y escaneos, se activan reglas para actividad de proceso NMAP, escaneo de vulnerabilidades por IPS (interno, en Colombia y externo), escaneo pesado de host TCP en puerto fijo, bloqueo de tráfico Cross-Site Scripting sobre portales web, detección de exploits de inicio de sesión en panel de control web, ataques de inyección SQL (interno, Colombia y externo), movimiento lateral detectado e intrusiones controladas por IPS en sus tres ámbitos.
- En detección de malware y amenazas, se identificaron reglas para conexiones de botnet (nivel interno, desde Colombia y desde redes externas), tráfico hacia URLs maliciosas (FortiGuard, listas CINS, Emerging Threats, listas SOC E&C), tráfico permitido hacia dominios de malware, Deep Web y redes anónimas, tráfico detectado desde IP de malware TweetFeed, detección de explotación Log4J y software espía detectado por IPS. En gestión de cuentas y privilegios, se parametrizaron reglas para modificación de directivas de grupo (GPO), usuarios agregados o eliminados de grupos de administradores, DNS, respaldo y escritorio remoto, creación y eliminación de usuarios Linux, cambio de contraseña en Windows y Linux, y enumeración de usuarios de Directorio Activo.
- En seguridad de sistemas operativos, se activaron reglas para modificación de permisos en servidores Linux (chmod, setuid, setgid, directorios grabables), modificación de módulos del kernel, servicios Windows inusuales, acceso sospechoso a extensiones de archivos confidenciales, inicio de sesión remoto de administrador (RDP), ejecución de PsExec como SISTEMA LOCAL, posible escalada de privilegios (enlace simbólico Osk/Command), volcado de contraseñas en LSASS y sesiones remotas PowerShell (WinRM).

	INFORME DE SEGUIMIENTO Y EVALUACIÓN (Trabajos de informes, seguimientos de ley y/o cumplimiento)	CÓDIGO:	F-AU-10
		VERSIÓN:	04
		VIGENCIA:	2025-06-12
	AUDITORÍA INTERNA	CLASIFICACIÓN:	IP

- **Resultado de la verificación documental:**

El total de 123 reglas activas permitió evidenciar que el sistema SIEM FortiSIEM dispone de capacidades de personalización y parametrización de reglas de correlación sobre el entorno de ENTerritorio S.A con cobertura sobre dispositivos de red, servidores Windows y Linux, Directorio Activo, aplicaciones web, servicios en nube (Office 365) y fuentes de inteligencia de amenazas de terceros (FortiGuard, CINS, Emerging Threats, TweetFeed, listas SOC E&C).

En consecuencia se identifica que el criterio **CUMPLE** conforme a lo indicado en el Anexo No. 2

D04-3

Criterios: ISO/IEC 27001:2022

A.8.15 – Registro de eventos

A.8.16 – Monitoreo

Criterio de verificación (Anexo Técnico No. 2, Numeral 4):

*"El SOC debe estar en capacidad de generar reportes e informes cuando el **supervisor del contrato lo requiera**. Los formatos de reportes soportados como mínimo serán .DOC, PDF, CSV y Texto Plano. Asimismo, deberá estar en capacidad de entregar a la entidad un **tablero de monitoreo de la ciberseguridad en tiempo real**."*

El servicio de SOC deberá contar con funcionalidades de análisis de comportamiento, detección avanzada de amenazas y respuesta a incidentes."

Con el propósito de verificar el cumplimiento del criterio contractual relativo al tablero de monitoreo de ciberseguridad en tiempo real, la Asesoría de Control Interno verificó los soportes documentales aportados por el GTI el 9 de septiembre de 2026, los cuales constan de 10 capturas de pantalla de los dashboards activos en la plataforma FortiSIEM v7.5.1.0620, organización Super, usuario admin.xx, con almacenamiento sobre EventDB en NFS (PT-D04-3-E1)

Los soportes referidos registran dos contextos diferenciados de monitoreo desplegados en la plataforma: El dashboard ENT-SOC, orientado a la seguridad de la información y la ciberseguridad, y el dashboard ENT-NOC, orientado al monitoreo de disponibilidad y rendimiento de la infraestructura tecnológica.

ENT-SOC presenta 11 pestañas especializadas, entre las cuales se verificaron: MONITOREO ELECCIONES 2026, Summary, IPs, Exploit, Web, Login/Chance, Users, Hunting, Office 365, FortiRecon y DLP.

Cada pestaña consolida en tiempo real indicadores específicos del estado de seguridad de la Sociedad, conforme se describe a continuación:

- i. Pestaña Summary: Presenta los incidentes activos clasificados por categoría (Seguridad: 824, Disponibilidad: 152, Rendimiento: 39, Otros: 1), y la tasa de ingesta en tiempo real de 1.455,04

 Empresa Nacional Promotora del Desarrollo Territorial S.A.	INFORME DE SEGUIMIENTO Y EVALUACIÓN (Trabajos de informes, seguimientos de ley y/o cumplimiento)	CÓDIGO:	F-AU-10
		VERSIÓN:	04
		VIGENCIA:	2025-06-12
	AUDITORÍA INTERNA	CLASIFICACIÓN:	IP

EPS (Events Per Second), valor que supera el umbral mínimo contractual de 1.000 EPS establecido en el Numeral 4 del Anexo Técnico No. 2.

Asimismo, se visualizan los principales casos de uso activos: SOC_ACCESOS_A_SITIOS_WEB_DENEGADOS (154 eventos), TCP_SCAN (68 eventos), TRAFICO_MALICIOSO_SOC_EYC (65 eventos), CAMBIO_UBICACION_USUARIO (57/35 eventos) y DNS_QUERY (33 eventos), junto con un evento de alta prioridad por cambio de configuración en FortiGate (FortiGate-event-chg-config: 1 evento HIGH).

- ii. Pestaña MONITOREO ELECCIONES 2026: Muestra el tráfico entrante por país de origen (Estados Unidos: 134.823 eventos; Brasil: 47.658 eventos) y las sesiones VPN exitosas por usuario (acastibl, cavila1, jestup, Irodrigu, marango), permitiendo la correlación georreferenciada de amenazas en el contexto del evento electoral nacional.

Se identificó la firma IPS signature-51391 con 1.964 eventos detectados. Los dispositivos con mayor tasa de generación de eventos fueron: FW_MAIN_CCP (435,69 EPS), FW_MAIN_CCB (266,29 EPS) y ENTSRVSQL01 (251,09 EPS).

- iii. Pestaña Exploit: Registra actividad de escaneo furtivo (Stealth Scan by IP V2.0) originado desde IPs de Estados Unidos, con los puertos más escaneados: UDP 3478 (2.257 eventos), TCP 443 (1.773 eventos) y UDP 53/DNS (1.631–1.626 eventos). Se evidenció bloqueo de acceso a servicios no autorizados para el usuario igalindxx (165 intentos a play.google.com).
- iv. Pestaña Web: Identifica comunicaciones hacia dominios maliciosos, en particular desde la IP interna 10.10.204.12 hacia zbshareware.net (2 eventos) y tptn0rhbtj.info (1 evento). Se registran bloqueos por categoría: Streaming (1.445 eventos) y Freeware (999 eventos), con mayor volumen de accesos denegados hacia p22-buy.itunes.apple.com (1.291 eventos).
- v. Pestaña Login/Chance: No registra inicios de sesión fallidos ni cambios de configuración en el período analizado. Se presentan accesos exitosos de red mediante los firewalls FW_MAIN_CCA y FW_MAIN_CCB para los usuarios FortiAIOPS (814/809 sesiones), cpulid (392), CMATEUS1 (324) y cmejia (308).
- vi. Pestaña Hunting: Consolida eventos de Microsoft 365 Entra ID (período 07 de septiembre de 2026, 06:57–09:47 a. m.) y tráfico de red entre nodos internos (172.16.x.xx → 172.16.x.xx: 3.640/2.724 eventos). Se detectan inicios de sesión fallidos de identidades privilegiadas: yviter (UserStrongAuthFailed, 22 intentos), xcorrea (UserDisabled, 15), mesadeayuda (IdsLocked, 10) y girlan (UserDisabled, 9). Adicionalmente, se registran comandos privilegiados fallidos en los servidores FONSRVRESPALD y procesos TiWorker.exe/TrustedInstaller.
- vii. Pestaña Office 365: Detecta inicio de sesión de Entra ID desde IPs externas 45.127.4xxx.x y 190.60.xx.xx (498 eventos cada una).

Se evidencia la cuarentena activa de 2 correos electrónicos de phishing dirigidos a las cuentas correspondencia.lira@enterritorio y xxx@enterritorio.gov.co, provenientes de info@deborahhamm.com, con asunto relacionado con elaboración de documentos mediante inteligencia artificial, clasificados en categoría Phish.

 Empresa Nacional Promotora del Desarrollo Territorial S.A.	INFORME DE SEGUIMIENTO Y EVALUACIÓN (Trabajos de informes, seguimientos de ley y/o cumplimiento)	CÓDIGO:	F-AU-10
		VERSIÓN:	04
		VIGENCIA:	2025-06-12
	AUDITORÍA INTERNA	CLASIFICACIÓN:	IP

- viii. Pestaña FortiRecon: Muestra resultados del monitoreo de superficie de ataque externa (EASM): se detectaron certificados digitales inválidos y cifrado TLS débil (Weak TLS Cipher) en el dominio enterpriseenrollment. (26 eventos cada uno, puerto 443, estado activo).

Adicionalmente, se identificaron credenciales filtradas en fuentes de inteligencia de amenazas (combo lists: 42.7kk Corp, 6kk Mailpass, Antipub, 12.3M Random, 5GB Mix) para las cuentas corporativas: xbultrag, xgalindo, agentemesa06, xxxdeplaneacion y xpinzon @enterritorio.gov.

Asimismo, se detectaron 8 vulnerabilidades activas en el servidor 20.206.xx.xx (puerto 4xx), correspondientes a los CVE: CVE-2007-3205, CVE-2013-2220, CVE-2025-14179, CVE-2026-14355, CVE-2026-17543, CVE-2026-6722, CVE-2026-6735 y CVE-2026-7259 (26 eventos activos cada uno).

- ix. Pestaña DLP: Registra eventos de prevención de pérdida de datos mediante la integración FortiDLP, con transferencias de archivos a través de Google Drive (drivefrontend-pa.clients6.google: 25 eventos; drive.google.com: 2 eventos), identificando las cuentas de usuario involucradas: xreinoso, (27 eventos), xruiz (2 eventos) xmendez (1 evento), mediante solicitudes HTTP POST desde el navegador Google Chrome.

Aspectos adicionales identificados:

El dashboard ENT-NOC complementa el monitoreo con pestañas de disponibilidad (UP-DOWN), memoria (RAM), procesamiento (CPU), almacenamiento (DISK) y monitoreo de URLs.

La pestaña UP-DOWN registra el estado de conectividad del firewall perimetral FW_MAIN (51 ms de latencia, último paquete 07/09/2026 09:44:47 a. m.) y los tiempos de disponibilidad de los servidores críticos: FONSRVHELISA02 (3 días), ENTSRVRADIUS, FONSRVDHCP01, FONSRVDC03 y FONSRVDHCP3 (8 días, 2 horas). Los indicadores de cumplimiento del ANS de disponibilidad muestran: fonsrvpuora12c (1 año 3 meses, 100%) y FW_MAIN_CCA (3 meses, 100%).

Resultado de la verificación documental:

Con base en lo anterior, se identificó que el contratista cuenta con un tablero de monitoreo de ciberseguridad en tiempo real, activo y operativo al momento de la verificación, que integra fuentes y capacidades de análisis (detección de amenazas avanzadas (FortiRecon), correlación de eventos de comportamiento (Hunting/Entra ID), prevención de pérdida de datos (DLP), monitoreo de aplicaciones en la nube (Office 365) y seguridad de endpoints, en cumplimiento de los requisitos establecidos en el Numeral 4 del Anexo Técnico No. 2.

En este sentido, se identificó que el criterio **CUMPLE** conforme con lo establecido en el Anexo No. 2.

- **D04-4**

ISO/IEC 27001:2022
A.8.16 – Monitoreo

Criterio de verificación (Anexo Técnico No. 2, Numeral 4):

 Empresa Nacional Promotora del Desarrollo Territorial S.A.	INFORME DE SEGUIMIENTO Y EVALUACIÓN (Trabajos de informes, seguimientos de ley y/o cumplimiento)	CÓDIGO:	F-AU-10
		VERSIÓN:	04
		VIGENCIA:	2025-06-12
	AUDITORÍA INTERNA	CLASIFICACIÓN:	IP

*SERVICIOS SOC – Num. 4: El contratista deberá prestar los servicios de ciberseguridad, SOC (Centro de Operaciones de Seguridad), **realizando seguimiento y análisis de la actividad de la red, servidores, puntos finales, bases de datos, aplicaciones y sitios web, en horario 7x24x365.***
//

La gestión de incidentes de seguridad se debe realizar mediante la herramienta de Gestión de incidentes de ENTerritorio S.A: se debe guardar registro de las acciones tomadas por el analista, los escalamientos y demás actividades realizadas, de forma que se pueda establecer una línea de tiempo del **incidente**.

La Asesoría de Control Interno efectuó la revisión de **13 informes mensuales SOC** aportados por el GTI, que cubren el período junio de 2025 a julio de 2026, distribuidos en dos proveedores, así:

No.	Período	Proveedor	Archivo	Sistema de tickets	Eventos escalados	Estado
1	Jun–Jul 2025	E&C Ingenieros SAS	INFORM2.DOC	Serie 39xxx	51	6 Pend / 45 Res
2	Jul–Ago 2025	E&C Ingenieros SAS	INFORM1.DOC	Serie 40xxx	49	10 Pend / 39 Res
3	Ago–Sep 2025	E&C → UT ENT 2027	IN2BDB1.DOC	Serie 40xxx–42xxx	49	43 Cerr / 6 Escal
4	27/Sep–26/Oct 2025	UT ENTerritorio 2027	IN24291.DOC	GLPI 42xxx–43xxx	44	43 Cerr / 1 Escal
5	Oct–Nov 2025	UT ENTerritorio 2027	INFORM4.DOC	GLPI 43xxx–44xxx	38	38 Cerr
6	Nov–Dic 2025	UT ENTerritorio 2027	INFORM3.DOC	GLPI 44xxx–45xxx	57	57 Cerr
7	27/Dic 2025–26/Ene 2026	UT ENTerritorio 2027	ENERO 2026.pdf	GLPI 45.547–46.571	69	59 Cerr / 10 Escal
8	27/Ene–26/Feb 2026	UT ENTerritorio 2027	FEBRERO 2026.pdf	GLPI 46.654–48.497	56	56 Cerr
9	27/Feb–26/Mar 2026	UT ENTerritorio 2027	MARZO 2026.pdf	GLPI (imagen)	28	28 Cerr
10	27/Mar–26/Abr 2026	UT ENTerritorio 2027	ABRIL 2026.pdf	TK-XXXX (imagen)	25	24 Cerr / 1 Escal
11	27/Abr–26/May 2026	UT ENTerritorio 2027	MAYO 2026.pdf	TK-XXXX (imagen)	27	27 Cerr
12	27/May–26/Jun 2026	UT ENTerritorio 2027	JUNIO 2026.pdf	Dual: SOC interno + Mesa Ayuda ENT (imagen)	15	15 Cerr
13	27/Jun–26/Jul 2026	UT ENTerritorio 2027	JULIO 2026.pdf	Dual: SOC + Mesa Ayuda ENT (imagen)	12	12 Cerr

 Empresa Nacional Promotora del Desarrollo Territorial S.A.	INFORME DE SEGUIMIENTO Y EVALUACIÓN (Trabajos de informes, seguimientos de ley y/o cumplimiento)	CÓDIGO:	F-AU-10
		VERSIÓN:	04
		VIGENCIA:	2025-06-12
	AUDITORÍA INTERNA	CLASIFICACIÓN:	IP

No.	Período	Proveedor	Archivo	Sistema de tickets	Eventos escalados	Estado
	TOTAL				524 eventos	

- **Análisis por eje de criterio:**

- i) Monitoreo 7x24x365 de red, servidores, endpoints, bases de datos, aplicaciones y sitios web

Respecto a la cobertura continua, se verificó para el período junio de 2025 a febrero de 2026, identificándose los siguientes registros que acreditan operación en franjas nocturnas, fines de semana y festivos:

- Actividad nocturna (00:00–06:00): Tickets registrados a las 0:15, 0:40, 1:20, 1:28, 1:30, 1:33, 1:40, 1:59, 2:09, 2:20, 2:40, 3:00, 3:08, 3:20, 3:30, 3:32, 3:35, 3:56, 4:00, 4:14, 4:15, 4:20, 4:33, 4:45, 4:59, 5:01, 5:10, 5:26, 5:30, 5:33, 5:40, 5:41, 6:05, entre otros, a lo largo de múltiples períodos.
- Festivos nacionales: Se confirma actividad el 25 de diciembre de 2025 (GLPI 45.516, 13:25) y el 1 de enero de 2026 (23:00), acreditando cobertura los días 25 y 1 de enero.
- Fines de semana: Tickets registrados los días sábado 27/12, 3/01, 10/01, 17/01, 24/01/2026 y sus respectivos domingos.

- ii) Gestión mediante la herramienta de gestión de incidentes de ENTerritorio S.A

Se identificaron tres etapas diferenciadas en el sistema de gestión de tickets a lo largo del período:

- Etapa 1 (Jun 2025 – Mar 2026): Sistema GLPI — herramienta del contratista. El criterio contractual exige el uso de la herramienta de ENTerritorio S.A . Durante esta etapa, que comprende 9 de los 13 informes, la gestión se realizó en una plataforma diferente a la de ENTerritorio S.A.
- Etapa 2 (Abr – May 2026): Se menciona el Sistema TK-XXXX.
- Etapa 3 (Jun – Jul 2026): Sistema dual: ticket interno del SOC + Mesa de Ayuda de ENTerritorio (formato Caso N.º XXXX / RF-XXXXXX-6-XXXX). Esta es la primera aparición de la herramienta de gestión de incidentes de ENTerritorio en la evidencia. Se documentó, entre otros, el evento por credencial comprometida (xxxx@enterritorio.gov.co), gestionado mediante Ticket SOC 6632 → Caso 2844 / RF-144763-6-2844.

- iii) Registro de acciones del analista y línea de tiempo del evento

Los informes mensuales presentan tablas de gestión de eventos con los campos: Fecha de apertura, ticket ID, tipo de alerta y estado final (Cerrado/Escalado/Pendiente).

Este nivel de detalle acredita la trazabilidad del estado del ticket, pero no permitió identificar el registro cronológico de acciones internas del analista como son: apertura → análisis → acciones tomadas → escalamiento → cierre), que es la condición que permite "establecer una línea de tiempo del evento y/o incidente".

	INFORME DE SEGUIMIENTO Y EVALUACIÓN (Trabajos de informes, seguimientos de ley y/o cumplimiento)	CÓDIGO:	F-AU-10
		VERSIÓN:	04
		VIGENCIA:	2025-06-12
	AUDITORÍA INTERNA	CLASIFICACIÓN:	IP

El soporte documental de los últimos 2 informes (junio y julio de 2026) identificó la integración con la Mesa de Ayuda de ENTerritorio S.A y referencia el seguimiento al Caso 2844, lo que sugiere mayor trazabilidad operativa, pero no aporta capturas del registro interno de acciones de ese caso.

- **Resultado de la verificación documental:**

Aspecto analizado	Observación
Continuidad del monitoreo 7x24x365	Confirmado para jun 2025–feb 2026.
Cobertura en festivos y fines de semana	Actividad documentada en Navidad (25/12/2025), Año Nuevo (1/01/2026) y fines de semana.
Uso de la herramienta de ENTerritorio S.A para gestión de incidentes	La Mesa de Ayuda de ENTerritorio S.A se identifica desde junio de 2026. Durante los primeros ~12 meses se usaron GLPI y TK-XXXX (herramientas del contratista).
Registro de acciones del analista y línea de tiempo	Los informes presentan estado final de tickets.
Escalamientos documentados	Los períodos documentan eventos escalados con estado de resolución.
Continuidad en la entrega de informes	13 informes consecutivos sin brechas para el período jun 2025 – jul 2026.

En consecuencia, se identifica que el criterio **CUMPLE**, respecto a lo indicado en el Anexo No. 2.

- **D04-5**

Criterios: ISO/IEC 27001:2022

8.16 – Monitoreo

Criterio de verificación (Anexo Técnico No. 2, Numeral 4):

“SERVICIOS SOC – Num. 4: La gestión de incidentes de seguridad se debe realizar mediante la herramienta de Gestión de incidentes de ENTerritorio S.A:

Se debe crear un ticket asignando: Número de incidente, criticidad, riesgo evaluado, alertas generadas y respuesta ante el mismo.

Se debe guardar registro de las acciones tomadas por el analista, los escalamientos y demás actividades realizadas, de forma que se pueda establecer una línea de tiempo del incidente. //

ANS – IMPACTO OPERATIVO (Num. 11): Escala de penalidades: Insignificante=10%, Menor=20%, Moderado=50%, Mayor=70%, Catastrófico=100% del valor mensual a facturar.”

Se analizaron los mismos 13 informes mensuales SOC del período junio 2025 – julio 2026, que fueron presentados por el GIT, en el criterio anterior.

Estos fueron analizados contra las exigencias específicas del criterio D04-5 del Anexo No.2 , con enfoque en:

- i) Los campos requeridos por ticket,

	INFORME DE SEGUIMIENTO Y EVALUACIÓN (Trabajos de informes, seguimientos de ley y/o cumplimiento)	CÓDIGO:	F-AU-10
		VERSIÓN:	04
		VIGENCIA:	2025-06-12
	AUDITORÍA INTERNA	CLASIFICACIÓN:	IP

ii) El registro de acciones del analista y

iii) Los indicadores de ANS con su escala de penalidades.

Se precisa que se efectuó el análisis documental por parte de la Asesoría de Control Interno, aun cuando fue certificado por el GTI, que no se presentaron incidentes en el periodo objeto de análisis. Lo anterior, con el propósito de identificar la gestión de tickets de la herramienta tecnológica utilizada por el contratista y la función de la supervisión al respecto.

- Análisis por eje de criterio:

i) Campos obligatorios del ticket:

El criterio exige que cada ticket contenga los siguientes campos: Número de incidente, criticidad, riesgo evaluado, alertas generadas y respuesta. La verificación de los 13 informes arrojó los siguientes resultados:

Campo requerido	Evidenciado en los informes	Observación
Número de incidente / ticket ID	Sí — en todos los periodos	GLPI series 39xxx–50xxx → TK-XXXX → Caso RF-XXXXXX según etapa
Criticidad por ticket	Parcial	Los informes presentan la severidad de eventos de forma agregada (Alto / Medio / Bajo) por periodo, no por ticket individual
Riesgo evaluado	No evidenciado	Ningún informe incluye columna de riesgo evaluado por ticket en las tablas de gestión
Alertas generadas (vinculadas al ticket)	Parcial	Se documentan las top 10 alertas por periodo y los casos de uso activos, pero sin vínculo sistemático a cada ticket individual
Respuesta ante el incidente	Parcial	El campo "Estado" (Cerrado / Escalado / Pendiente) refleja el resultado, no el detalle de la respuesta ejecutada

ii) Registro de acciones del analista y línea de tiempo del incidente

Los informes presentan tablas de gestión de eventos con los campos: Fecha, ticket ID, tipo de alerta y estado final.

Esta estructura acredita la trazabilidad del estado de cierre, pero no incluye el historial de acciones cronológicas internas (apertura → análisis → acciones tomadas → escalamiento → cierre) que el Anexo Técnico requieren para "establecer una línea de tiempo del incidente."

Se identifica un elemento favorable a partir de junio de 2026: El informe documenta la gestión del evento / incidente de credencial comprometida (xxxx@enterritorio.gov.co) con trazabilidad entre sistemas (Ticket SOC 6632 → Caso 2844 / RF-144763-6-2844 Mesa de Ayuda ENTerritorio).

Este es el único caso de la evidencia aportada por el GTI que presenta vinculación entre el evento detectado y el registro en la herramienta de ENTerritorio S.A, pero sin que se aporten capturas del historial interno del caso.

 Empresa Nacional Promotora del Desarrollo Territorial S.A.	INFORME DE SEGUIMIENTO Y EVALUACIÓN (Trabajos de informes, seguimientos de ley y/o cumplimiento)	CÓDIGO:	F-AU-10
		VERSIÓN:	04
		VIGENCIA:	2025-06-12
	AUDITORÍA INTERNA	CLASIFICACIÓN:	IP

A partir de abril de 2026, los informes incorporan una sección denominada "Gestión de incidentes formales" (referenciada bajo procedimiento SIC-PR-03 y formato SIC-FT-05), reportando 0 incidentes materializados en los meses de abril, mayo, junio y julio de 2026.

Esto indica que el contratista distingue entre alertas/eventos gestionados por ticket SOC e incidentes formales según su procedimiento interno, aunque dicho procedimiento no fue aportado como soporte documental por el GIT.

iii). ANS – Impacto Operativo y escala de penalidades

A continuación se presenta lo identificado en los soportes documentales:

Período	Incidentes materializados	ANS documentado	Penalidad aplicable
Jun 2025 – Mar 2026	No se segrega en los informes	No extraíble — referenciado como objetivo	No evidenciado
Abr 2026	0 (SIC-PR-03)	No como tabla numérica	0 (sin incidente)
May 2026	0 (SIC-PR-03, SIC-FT-05)	No como tabla numérica	0 (sin incidente)
Jun 2026	0 formal (1 incidente gestionado)	No como tabla numérica	Pendiente de clasificación
Jul 2026	0 (SIC-PR-03)	No como tabla numérica	0 (sin incidente)

Conforme a lo anterior, se identificó que el criterio **CUMPLE PARCIALMENTE**. Lo anterior, se indica teniendo en cuenta aspectos de mejora continua documental de la herramienta utilizada para los tickets de eventos e incidentes, que deben ser analizados por el supervisor en conjunto con el proveedor.

- D04-6

Criterios: A.5.24 – A.5.28 de ISO/IEC 27001:2022.

Criterio de verificación (Anexo Técnico No. 2, Numeral 4):

“SERVICIOS SOC – Num. 4: Proveer un servicio de análisis forense para los casos en que sea necesario investigar incidentes informáticos.

Los procedimientos de investigación deberán estar en concordancia con la norma ISO/IEC 27037 y la legislación vigente en Colombia. Se estiman 2 análisis por año, sin límite a la cantidad de veces que se requiera.”

Este aspecto no fue verificado, dado que no se han presentado incidentes que requieran el servicio de análisis forense, tal como lo indica el Anexo No. 2

Al respecto se precisa lo indicado por GTI en el Memorando 202615010002183 del 9 de septiembre de 2026:

***“ 2. (...) Inexistencia de Incidentes y Delimitación del Servicio Forense.
Frente a la solicitud de “2. Informes de análisis forense con cadena de custodia documentada (...) conforme a ISO/IEC 27037:2012” nos permitimos certificar que durante***

	INFORME DE SEGUIMIENTO Y EVALUACIÓN (Trabajos de informes, seguimientos de ley y/o cumplimiento)	CÓDIGO:	F-AU-10
		VERSIÓN:	04
		VIGENCIA:	2025-06-12
	AUDITORÍA INTERNA	CLASIFICACIÓN:	IP

el periodo objeto d evaluación (julio 2025 a julio 2026) no se presentó ni materializó ningún incidente de seguridad de la información de criticidad Moderada, Mayor o Catastrófica en la plataforma tecnológica de la entidad.

El Anexo Técnico No. 2 estipula que este servicio se activará bajo demanda “para los casos en que sea necesario investigar incidentes informáticos”. En consecuencia, al registrarse un total de cero (0) eventos críticos, los informes forenses y los registros de cadena de custodia asociados no fueron requeridos ni generados en la operación real.” Negrilla de la Asesoría de Control Interno.” (negrilla de la Asesoría de Control Interno).

- D04-7

Criterios: ISO/IEC 27001:2022

A.8.16 – Monitoreo

Criterio de verificación (Anexo Técnico No. 2, Numeral 4):

“ANS – Num. 11: DISPONIBILIDAD SERVICIO DE SEGURIDAD (Infraestructura / Networking / SOC / Certificados / Antimalware / DLP / NAC / Seguridad Web): La indisponibilidad es el número total de minutos, durante el mes contratado, en los que el servicio no está disponible o funcional en su totalidad.

Los resultados del monitoreo son mantenidos por el contratista para consulta de ENTerritorio S.A en cualquier momento. // PENALIDAD POR IMPACTO: Insignificante=10%, Menor=20%, Moderado=50%, Mayor=70%, Catastrófico=100% del valor mensual a facturar (antes de IVA).”

El Anexo Técnico No. 2 (incorporado mediante Adenda No. 1) establece que el contratista debe realizar mensualmente conciliaciones de facturación con ENTerritorio S.A., en las que se validen los servicios prestados y se apliquen las penalizaciones por incumplimiento de Acuerdos de Nivel de Servicio (ANS) a que haya lugar.

Estas reuniones deben documentarse en Actas de Reunión bajo el formato F-DO-06 Versión 03 (Gestión Documental), firmadas por el Gerente de Proyecto y por el Gerente del Grupo de Tecnologías de la Información de ENTerritorio S.A.

Cada Acta de Conciliación de ANS debe incluir:

- Análisis de ANS de Operación por línea de servicio,
- Análisis de ANS para Notificaciones y Documentación,
- Resumen de facturación del período con discriminación por las 8 líneas de servicio,
- Tabla de descuentos ANS aplicados por línea, y
- Firmas de aprobación de ambas partes.

	INFORME DE SEGUIMIENTO Y EVALUACIÓN (Trabajos de informes, seguimientos de ley y/o cumplimiento)	CÓDIGO:	F-AU-10
		VERSIÓN:	04
		VIGENCIA:	2025-06-12
	AUDITORÍA INTERNA	CLASIFICACIÓN:	IP

Conforme a los soportes documentales se verificaron 12 Actas de Conciliación de ANS correspondientes al período auditado (julio 2025 — julio 2026), identificadas como Actas No. 15 a 26, todas bajo el formato F-DO-06 Versión 03 — Vigencia 2023-07-31.

Acta No.	Período de facturación	Fecha reunión	ANS Operación (antes de IVA)	ANS Notif./Doc. (antes de IVA)	Total factura (con IVA)	Firmado ENTerritorio
15	27-Jul al 26-Ago-2025	02-Sep-2025	\$0,00	\$0,00	\$990.702.215,54	2025.09.15
16	27-Ago al 26-Sep-2025	01-Oct-2025	\$0,00	\$0,00	\$996.476.317,10	2025.10.21
17	27-Sep al 26-Oct-2025	29-Oct-2025	\$0,00	\$0,00	\$956.643.221,11	2025.11.13
18	27-Oct al 26-Nov-2025	02-Dic-2025	\$3.009.831,93	\$0,00	\$988.048.764,58	2025.12.05
19	27-Nov al 26-Dic-2025	30-Dic-2025	\$0,00	\$0,00	\$957.214.681,57	2026.01.15
20	27-Dic-2025 al 26-Ene-2026	29-Ene-2026	\$0,00	\$0,00	\$959.029.023,59	2026.02.09
21	27-Ene-2026 al 26-Feb-2026	09-Mar-2026	\$0,00	\$0,00	\$999.023.081,62	2026.03.12
22	27-Feb al 26-Mar-2026	01-Abr-2026	\$0,00	\$0,00	\$969.987.730,55	2026.04.10
23	27-Mar al 26-Abr-2026	27-Abr-2026	\$0,00	\$0,00	\$981.003.778,62	2026.05.25
24	27-Abr al 26-May-2026	26-May-2026	\$0,00	\$0,00	\$1.016.228.424,56	2026.06.xx
25	27-May al 26-Jun-2026	02-Jul-2026	\$0,00	\$0,00	\$1.140.853.207,16	2026.07.14
26	27-Jun al 26-Jul-2026	28-Jul-2026	\$0,00	\$0,00	\$1.090.995.259,50	2026.08.19
TOTALS	12 Actas (No. 15 – 26)	Jul 2025 – Jul 2026	\$3.009.831,93	\$0,00	Ver detalle	12/12

- Resultado de la verificación documental

i). Se verificó la existencia de las 12 Actas de Conciliación de ANS correspondientes al período comprendido entre el 27 de julio de 2025 y el 26 de julio de 2026 (Actas No. 15 a 26).

La totalidad de los documentos se encuentran disponibles en el repositorio del contrato, suscritos mediante el formato F-DO-06 Versión 03, con la estructura estándar que incluye: Objetivos de la reunión, seguimiento a compromisos anteriores, desarrollo por líneas de servicio, análisis ANS de operación, análisis ANS para notificaciones y documentación, resumen de facturación, descuentos ANS por línea de servicio, aprobaciones y firmas.

ii). Análisis ANS — Penalizaciones aplicadas

	INFORME DE SEGUIMIENTO Y EVALUACIÓN (Trabajos de informes, seguimientos de ley y/o cumplimiento)	CÓDIGO:	F-AU-10
		VERSIÓN:	04
		VIGENCIA:	2025-06-12
	AUDITORÍA INTERNA	CLASIFICACIÓN:	IP

De las 12 Actas revisadas, 11 registran descuento total por ANS de \$0,00 tanto en Operación como en Notificaciones y Documentación, lo que indica pleno cumplimiento de los niveles de servicio en dichos períodos.

Únicamente el Acta No. 18 (período 27-Oct al 26-Nov-2025) registró un descuento ANS por Operación, derivado del siguiente incidente:

PENALIZACIÓN ANS ACTA 18	
Línea afectada	Línea 6 — Servicios de Canales de Comunicación (Canal CCP)
Evento	Falla en descubrimiento de DNS públicos — 09 de noviembre de 2025, 05:30 a.m. a 01:30 p.m.
Tiempo de indisponibilidad	8 horas × 60 minutos = 480 minutos
Disponibilidad real	(43.200 min – 480 min) / 43.200 min = 98,889%
Umbral contractual	99,70% (tabla de penalización Anexo Técnico — Línea 6)
Penalización aplicada	100% del valor del Canal CCP = \$3.009.831,93 antes de IVA
Impacto en factura	Valor sin penalización (Línea 6): \$43.735.798,32 Valor con penalización: \$40.725.966,39 Total factura Acta 18 con IVA: \$988.048.764,58
Descuento ANS total Acta 18	\$3.009.831,93 antes de IVA (solo Operación; Notificaciones y Documentación: \$0)
Observación	Se tomaron medidas de mitigación con VPN durante el lapso de falla. La penalización fue aceptada y aplicada por la UT en la factura del período.

iii) Oportunidad y firma de las Actas

Todas las Actas presentan firmas de aprobación de ambas partes: el Gerente de Proyecto (firma manuscrita) y el Gerente del Grupo de Tecnologías de la Información de ENTerritorio S.A. — firma digital certificada).

Las reuniones se realizaron mediante la plataforma Microsoft Teams. No se identificaron Actas sin firmar ni compromisos pendientes de cumplimiento.

iv). Aspectos adicionales observados

A partir del Acta No. 22 (período Feb-Mar 2026) se registra la incorporación de 50 Licencias E1 de Office 365, aprobadas por el Gerente GTI el 24 de marzo de 2026. Estas licencias fueron activadas de forma inmediata en el tenant de ENTerritorio S.A.

A partir del Acta No. 23 (período Mar-Abr 2026), la actividad de la Mesa Integral de Servicio incluye un incremento adicional de \$10.000.000 (tercer pago fraccionado) por concepto de horas extra y tiempo adicional nocturno 7×24 prestado en los meses de diciembre 2025, enero 2026 y febrero 2026 (Cierre Contable Presupuestal 2025 y Proceso de Contratación 2026). El valor se distribuyó en tres cuotas iguales (Actas 23, 24 y 25).

En consecuencia a lo analizado, se identifica que el criterio **CUMPLE**, conforme a lo establecido en el Anexo No. 02.

	INFORME DE SEGUIMIENTO Y EVALUACIÓN (Trabajos de informes, seguimientos de ley y/o cumplimiento)	CÓDIGO:	F-AU-10
		VERSIÓN:	04
		VIGENCIA:	2025-06-12
	AUDITORÍA INTERNA	CLASIFICACIÓN:	IP

- **Seguimiento a las obligaciones del supervisor contractual GTI:**

N.º	Componente / Dimensión	Descripción y Obligaciones Principales	Norma / Marco Aplicable
★	Seguimiento a Obligaciones del Supervisor Contractual	Supervisor: Armando Vivas Salamanca (Gerente GTI - ENTerritorio) Verificar el cumplimiento de las funciones de supervisión conforme al Manual M-PR-01 v2: · Revisión y aprobación de informes del contratista · Control de ANS (disponibilidad e impacto operativo) · Registro y seguimiento de actas de seguimiento · Gestión de incidentes y aplicación de penalidades · Verificación de obligaciones técnicas y laborales del contratista	M-PR-01 v2 – Manual de Supervisión Contractual ENTerritorio Estatuto General de Contratación (Ley 80/1993, Art. 84) NOGAJ 2024 – Principios 13 a 15 (criterios de riesgo, relevancia y materialidad) Contrato No. 2024612 – Cláusulas de supervisión

- **III-1. Visitas de verificación a la infraestructura física — Centros de Cómputo CCP y CCA**

Criterio de verificación (Anexo Técnico No. 2 – Numeral 1, según Adenda No. 1):

"El contratista deberá disponer de la infraestructura tecnológica requerida para la prestación de los servicios de Infraestructura como Servicio (IaaS), la cual deberá estar alojada en centros de cómputo con las condiciones de seguridad física, disponibilidad y redundancia necesarias para garantizar la continuidad operativa de ENTerritorio S.A.

*La infraestructura deberá contar con un Centro de Cómputo Principal (CCP) y un Centro de Cómputo Alterno (CCA), **debidamente certificados y en operación durante la vigencia del contrato.***

Con el propósito de verificar el cumplimiento de las obligaciones contractuales relacionadas con la disponibilidad y operación de la infraestructura física de los centros de cómputo que soportan los servicios de ENTerritorio S.A., la Asesoría de Control Interno revisó las actas de visita suscritas durante la ejecución del Contrato, correspondientes a los centros de cómputo CCP (Centro de Cómputo Principal — Data Center Torre Central, Bogotá) y CCA (Centro de Cómputo Alterno — Datacenter Globenet Barranquilla), conforme se detalla a continuación:

i) Centro de Cómputo Alterno (CCA) — Datacenter IFX Globenet, Barranquilla:

Se verificaron soportes documentales de las 3 visitas realizadas al CCA, las cuales documentan la evolución de la infraestructura desde el inicio del contrato hasta la vigencia 2025, así:

- La primera visita (Acta CCA-001, 09/07/2024) tuvo como objetivo el reconocimiento de la infraestructura física del Datacenter Globenet Barranquilla para el ambiente de Contingencia de

 Empresa Nacional Promotora del Desarrollo Territorial S.A.	INFORME DE SEGUIMIENTO Y EVALUACIÓN (Trabajos de informes, seguimientos de ley y/o cumplimiento)	CÓDIGO:	F-AU-10
		VERSIÓN:	04
		VIGENCIA:	2025-06-12
	AUDITORÍA INTERNA	CLASIFICACIÓN:	IP

ENTerritorio S.A., con participación del Oficial de Seguridad Informática de Enterritorio S.A., la Gerente de Proyecto Implementación Línea IAAS, y el proveedor del contrato.

En los soportes documentales se indicó que durante esta visita se validaron las certificaciones con que cuenta el Data Center y el cumplimiento de normativas vigentes, así como los espacios asignados para los equipos de la solución. Se programó una segunda visita para el 12 de septiembre de 2024 (PT-III-1-E1).

- La segunda visita (Acta CCA-002, 12/09/2024) permitió a los asistentes confirmar la documentación presentada y validar el inventario físico de equipos instalados en los racks del CCA, con asistencia adicional del Oficial de Seguridad del contrato y el Líder Técnico,

Se verificaron los siguientes componentes activos de acuerdo a los soportes documentales: Servidor VMware (cobagbllx04, Dell R550, serial D98RWP3, Rack ZIR6A U21), servidor KVM (cobagbllx05, Dell R550, serial G98RWP3, Rack ZIR6A U22), Balanceador de Aplicaciones (Kemp LM-XHC55-NG, serial TSCE32000564, Rack ZIR1A U15) y Firewall perimetral (FW-400-CCA, Fortinet Fortigate 400F, serial FG4H0FT923906328, Rack ZIR1A U14).

Se establecieron compromisos para la entrega funcional del CCA (25/09/2024), evidencias de aplicaciones alojadas (26/09/2024) y pruebas de velocidad y conmutación de canales (03/10/2024) (PT-III-1-E2).

- La tercera visita (Acta CCA-003, 19/11/2025) permitió evidenciar la actualización del inventario de equipos del CCA con los componentes en operación al momento de la verificación: servidor VMware (cobagbllx04, Dell R640, serial D98RWP3, Rack ZIR7A U21), servidor KVM (cobagbllx05, Dell R640, serial D4VHK44, Rack ZIR6A U22), Balanceador de Aplicaciones (Kemp LM-XHC55-NG, serial TSCE32000564, Rack ZIR2A U18-19) y Firewall perimetral (FW-400-CCA, Fortinet Fortigate 400F, serial FG4H0FT923906328, Rack DC201AR20 U15).

Se evidenció que el Datacenter se encontraba en ejecución de obras civiles en la zona contigua al cuarto de equipos, lo que generaba condiciones de polvo y suciedad en los racks. En consecuencia, se estableció como compromiso la limpieza de los equipos por parte del Datacenter Globenet una vez concluidas las obras, con fecha de cumplimiento de febrero de 2026.

La conclusión del acta registra la validación satisfactoria del Datacenter para la infraestructura CCA de ENTerritorio S.A. Nota: Por políticas de seguridad del Datacenter IFX GLOBENET Barranquilla no fue posible obtener registros fotográficos; esta condición es reportada expresamente en el acta (PT-III-1-E3)

iii) Centro de Cómputo Principal (CCP) — Datacenter Torre Central IFX, Bogotá:

La visita al CCP (Acta CCP-003, 13/11/2025) tuvo por objeto la auditoría de los equipos activos que soportan las soluciones tecnológicas de ENTerritorio S.A. para los ambientes de Producción, Pruebas y Desarrollo, en el marco del Contrato.

Participaron el profesional de Apoyo Redes e IPv6, ENTERRITORIO S.A., el Oficial de Continuidad, y el Líder Técnico del proveedor.

 Empresa Nacional Promotora del Desarrollo Territorial S.A.	INFORME DE SEGUIMIENTO Y EVALUACIÓN (Trabajos de informes, seguimientos de ley y/o cumplimiento)	CÓDIGO:	F-AU-10
		VERSIÓN:	04
		VIGENCIA:	2025-06-12
	AUDITORÍA INTERNA	CLASIFICACIÓN:	IP

El ingreso al Data Center ubicado en el edificio Torre Central (Av. El Dorado # 68C-61, Piso 5) se surtió mediante 5 filtros de seguridad: validación en recepción del edificio (1°), tarjeta de acceso exclusiva al Piso 5 (2°), recepción del Data Center (3°), asignación de personal de acompañamiento (4°) y acceso al contenedor específico de los racks (5°).

Se realizó apertura de los racks B_R23, B_R24 y B_R25, verificando el siguiente inventario de componentes en operación:

Nombre del Elemento	Rack	U	Tipo	Marca	Modelo	Serial	Finalidad
FW-400-CCP-1	B_R23	U42	Firewall	Fortinet	Fortigate 400F	FG4H0FT923906324	Seguridad Perimetral Master
FW-400-CCP-2	B_R23	U41	Firewall	Fortinet	Fortigate 400F	FG4H0FT923906339	Seguridad Perimetral Slave
MIKROTIK_PPL	B_R23	U39	Router	Mikrotik	CCR2004-16G-2S+	HGG09XJHRS7\R2	Conectividad PPL
MIKROTIK_BACKUP	B_R23	U38	Router	Mikrotik	CCR2004-16G-2S+	HGG09TD5D8F\R2	Conectividad Backup
cobogdtcdtx27	B_R23	U22	Servidor	DELL	R660	G4VHK44	Servidor VMware
cobogdtcdtx33	B_R23	U17	Servidor	DELL	R660	HUVHK44	Servidor VMware
BALANCEADOR 1	B_R23	U35-34	Balanceador	Kemp	LM-XHC55-NG	TSCE32000554	Balanceador Aplicaciones Master
BALANCEADOR 2	B_R23	U33-32	Balanceador	Kemp	LM-XHC55-NG	TSCE32000561	Balanceador Aplicaciones Slave
LIBRERÍA	B_R23	U3-1	Librería	Dell	EMC ML3	3555L3A78-02AVH	Librería Cintas Backup
SW CORE 1	B_R24	U39	Switch	Juniper	QFX5120-32C	TA3715340174	SW Core 1 – Virtualización
cobogdtcdtx163	B_R24	U17	Servidor	DELL	R640	G34CKQ3	Servidor BD SQL
cobogdtcdtx41	B_R24	U15	Servidor	DELL	R640	D9CTPX2	Servidor KVM
cobogdtcdtx43	B_R24	U16	Servidor	DELL	R640	CFMV4K3	Servidor KVM
SW CORE 2	B_R25	U41	Switch	Juniper	QFX5120-32C	VF3122210181	SW Core 2 – Virtualización

 Empresa Nacional Promotora del Desarrollo Territorial S.A.	INFORME DE SEGUIMIENTO Y EVALUACIÓN (Trabajos de informes, seguimientos de ley y/o cumplimiento)	CÓDIGO:	F-AU-10
		VERSIÓN:	04
		VIGENCIA:	2025-06-12
	AUDITORÍA INTERNA	CLASIFICACIÓN:	IP

Nombre del Elemento	Rack	U	Tipo	Marca	Modelo	Serial	Finalidad
cobogdtcdtx108	B_R2 5	U17	Servidor	DELL	R640	63KJSZ2	Servidor BD SQL
Almacenamiento	D_R5 9	25- 26	Almacenamiento	IBM	STORWIZE V7000 G3	78E03CF	Storage 100 TB

El administrador del Datacenter IFX brindó información sobre las certificaciones del Data Center Júpiter, la redundancia de componentes de infraestructura y el modelo de operación.

Se revisó adicionalmente el equipo de almacenamiento IBM Storwize V7000 G3 (serial 78E03CF), instalado en zona diferenciada del Data Center para protección de datos.

No se registraron compromisos pendientes. La conclusión del acta registra la validación satisfactoria del Datacenter para la infraestructura CCP de ENTerritorio S.A. (PT-III-1-E4).

Con base en las 4 actas de visita revisadas, se identificó que el contratista mantiene operativos tanto el Centro de Cómputo Principal (CCP — Torre Central, Bogotá) como el Centro de Cómputo Alterno (CCA — Globenet, Barranquilla), con equipamiento físico inventariado, seriales verificados e infraestructura de seguridad perimetral, virtualización, balanceo de aplicaciones y almacenamiento debidamente instalados y validados en visitas presenciales conjuntas con la supervisión de ENTerritorio S.A.

Frente a lo anterior, se identifica que el criterio del Anexo No. 2, **CUMPLE**.

III-2. Gestión de incidentes (P-RI-19) y aprobación de plantillas de hardening / plan de actualización por vigencia

Criterio de verificación (Anexo Técnico No. 2):

*“NETWORKING – Num. 3: **En caso de la materialización de un riesgo**, el CONTRATISTA, en coordinación con el Supervisor del Contrato o quien este designe, debe actuar como primer respondiente acorde al procedimiento P-RI-19 GESTIÓN DE INCIDENTES. //*

HARDENING (Num. 2): Las plantillas de hardening deben ser aprobadas por el supervisor del contrato. //

El supervisor debe aprobar el plan de actualización al inicio de cada vigencia. Supervisión activa implica comunicación formal de incumplimientos.”

Frente al criterio, el GTI indicó lo siguiente en su respuesta del 17 de septiembre de 2026:

“(…) el ciclo de hardening es una tarea recurrente que se ejecuta en la medida en que surgen las alertas de ciberseguridad, asimismo se tiene un ciclo básico de actualizaciones mínimo de tres meses, todas las actualizaciones se aprueban en comité de cambios. en el periodo solicitado

	INFORME DE SEGUIMIENTO Y EVALUACIÓN (Trabajos de informes, seguimientos de ley y/o cumplimiento)	CÓDIGO:	F-AU-10
		VERSIÓN:	04
		VIGENCIA:	2025-06-12
	AUDITORÍA INTERNA	CLASIFICACIÓN:	IP

fueron 25 actualizaciones de Hardening, Firewall y Red Wifi (la controladora esta embebida en el FW) al menos 12 actualizaciones, Switches 1 actualización en el periodo”

De la revisión de las actas de seguimiento contractual de las vigencias 2025 y 2026, la Asesoría de Control Interno no identificó situaciones que constituyan materialización de riesgo en los términos del Numeral 3 del Anexo Técnico No. 2, que hubiera activado la obligación del contratista de actuar como primer respondiente bajo el procedimiento P-RI-19 GESTIÓN DE INCIDENTES.

Las situaciones registradas en las Actas No. 15-2026 y No. 16-2026 corresponden, en un caso, a una solicitud de la Sociedad de un reporte sobre novedades con los servicios de Certicámara y FVC (sin que conste la declaración formal de materialización de un riesgo), y en el otro, a comunicados informativos de COLCERT sobre recomendaciones de configuración de herramientas de seguridad, los cuales no equivalen a la ocurrencia de un incidente en el sentido contractual.

Asimismo, tal como ya se indicó, el GTI en el Memorando 202615010002183 del 9 de septiembre de 2026, especificó:

“ 2. (...) Inexistencia de Incidentes y Delimitación del Servicio Forense.

Frente a la solicitud de “2. Informes de análisis forense con cadena de custodia documentada (...) conforme a ISO/IEC 27037:2012” nos permitimos certificar que durante el periodo objeto d evaluación (julio 2025 a julio 2026) no se presentó ni materializó ningún incidente de seguridad de la información de criticidad Moderada, Mayor o Catastrófica en la plataforma tecnológica de la entidad.” (Negrilla de la Asesoría de Control Interno)” (negrilla Asesoría de Control Interno)

En el marco de lo anterior, el criterio se identifica en estado: **CUMPLE.**

- III-3

ISO/IEC 27001:2022

Cláusula 10.1 – Acción correctiva y su eficacia

Criterio de verificación (Anexo Técnico No. 2):

“HARDENING (Num. 2): El Contratista debe presentar las plantillas de hardening para cada sistema. Estas deben ser aprobadas por el supervisor del contrato. //

ACTUALIZACIÓN (Num. 2): El plan de actualización debe ser presentado al supervisor del contrato y aprobado por este al inicio de cada vigencia. [El ciclo completo supervisor → requerimiento → respuesta contratista → verificación supervisor es obligación implícita del ejercicio de supervisión.”

El Anexo Técnico No. 2 del Contrato, establece que el proveedor debe presentar al supervisor del contrato un plan de actualización de los sistemas bajo su responsabilidad, el cual debe ser aprobado por dicho supervisor al inicio de cada vigencia contractual.

 Empresa Nacional Promotora del Desarrollo Territorial S.A.	INFORME DE SEGUIMIENTO Y EVALUACIÓN (Trabajos de informes, seguimientos de ley y/o cumplimiento)	CÓDIGO:	F-AU-10
		VERSIÓN:	04
		VIGENCIA:	2025-06-12
	AUDITORÍA INTERNA	CLASIFICACIÓN:	IP

El criterio evalúa que dicho plan haya sido elaborado, presentado oportunamente y que las actividades de actualización consignadas en el mismo se hayan ejecutado y registrado de forma trazable.

El GTI de ENTerritorio S.A. indicó que la evidencia de ejecución del plan de actualización para el período auditado corresponde al Reporte de Cambios registrados en la herramienta ARANDA, el cual es el mismo soporte documental presentado para el criterio III-2 (Hardening). Este reporte contiene el registro de todos los cambios ejecutados a la infraestructura tecnológica del contrato durante el período Jul-2025 a Jul-2026.

- **Análisis por eje de criterio:**

De los soportes documentales aportados, se revisó el "Reporte de Cambios en Aranda 2025–2026", el reporte comprende un total de 11.215 registros de casos (CAMBIO, INCIDENTE y REQUERIMIENTO DE SERVICIO) con fecha de registro entre el 1 de julio de 2025 y el 31 de julio de 2026.

Para efectos del presente criterio se analizaron los 128 casos de tipo CAMBIO, de los cuales 57 corresponden a cambios directos sobre la infraestructura tecnológica (categorizados bajo "Control de Cambios de Infraestructura Tecnológica" y "Azure") y 71 corresponden a solicitudes de cambio de servicio (SLA "Estándar").

Tabla 4 Resumen global del reporte de cambios (casos tipo CAMBIO)

Tipo de cambio	Registros	Cerrados / Anulados	Cumplimiento ANS
Cambios de Infraestructura Tecnológica	57	57 cerrados (0 pendientes)	100% DENTRO
Solicitudes de cambio (SLA Estándar)	71	68 cerradas / 1 anulada / 2 en trámite	100% DENTRO (cerrados)
TOTAL CAMBIOS	128	125 cerrados / 1 anulado / 2 en trámite	0 FUERA de ANS

Tabla 5 Cambios de Infraestructura Tecnológica por mes (Jul-2025 a Jul-2026)

Mes	Azure	Servidores Virtuales	Firewalls	Seg. Perimetral / WAF	Amb. Prod. / Pruebas	Otros	Total
Jul-2025	4	2	2	1	1	—	10
Ago-2025	3	5	—	—	—	—	8
Sep-2025	2	3	—	—	1	1	7
Oct-2025	4	4	—	—	—	1	9
Nov-2025	1	4	—	—	—	1	6
Dic-2025	2	3	1	—	—	—	6
Ene-2026	—	—	—	—	—	—	0
Feb-2026	—	—	—	—	1	—	1
Mar-2026	1	—	—	—	—	—	1
Abr-2026	1	—	—	—	—	—	1
May-2026	—	—	—	—	—	1	1
Jun-2026	2	—	—	—	2	—	4
Jul-2026	3	—	—	—	—	—	3
TOTAL	23	21	3	3	7	3	57

Nota: "Otros" incluye Herramientas de Análisis de Seguridad, Unidades de Almacenamiento. "—" indica 0 registros en ese mes.

	INFORME DE SEGUIMIENTO Y EVALUACIÓN (Trabajos de informes, seguimientos de ley y/o cumplimiento)	CÓDIGO:	F-AU-10
		VERSIÓN:	04
		VIGENCIA:	2025-06-12
	AUDITORÍA INTERNA	CLASIFICACIÓN:	IP

Como ya se indicó, el GTI ENTerritorio S.A. señaló que la evidencia correspondiente al criterio III-3 (Plan de Actualización) es la misma que la presentada para el criterio III-2 (Hardening): el Reporte de Cambios registrados en la herramienta ARANDA para el período julio 2025 — julio 2026. Esto implica que la evidencia de ejecución de las actualizaciones de sistemas se encuentra contenida en los tickets de tipo CAMBIO registrados en dicha herramienta de gestión de servicios de TI.

El Reporte Aranda evidenció la ejecución de 57 cambios directos sobre infraestructura tecnológica durante el período auditado.

Las categorías de los cambios reflejan actividades de actualización en los principales componentes del contrato: plataforma Azure (23 cambios — aplicación de parches de seguridad y mitigación de vulnerabilidades), Servidores Virtuales (21 cambios — actualizaciones y hardening de sistemas), Firewalls (3 cambios — actualizaciones de versiones de firmware), y demás componentes de seguridad perimetral, WAF, almacenamiento y ambientes de producción/pruebas.

De los 57 cambios de infraestructura registrados, la totalidad fueron gestionados dentro del ANS contractual ("ANS Cambios a la Infraestructura Tecnológica"), sin ningún caso reportado como fuera de ANS.

Los 68 casos de solicitudes de cambio cerrados también reportan cumplimiento dentro del ANS y 2 casos en estado "Registrado" (solicitudes de cambio No. 2331 — ene-2026 y No. 2401 — may-2026) no cuentan con un cierre formal en el sistema, por lo que se recomienda verificar su estado. El caso No. 2161 fue anulado por solicitud del usuario.

- **Resultado de la verificación documental**

El criterio III-3 del Anexo Técnico No. 2, exige que el plan de actualización sea presentado al supervisor del contrato y aprobado por este al inicio de cada vigencia.

La evidencia aportada (Reporte Aranda) corresponde a registros de ejecución de cambios a lo largo del período, no a un documento formal de plan de actualización presentado y aprobado previo al inicio de las vigencias 2025 y 2026. No obstante, los registros en Aranda evidencian que las actualizaciones fueron gestionadas de forma sistemática, trazable y dentro de los tiempos de atención y solución contractuales, lo que refleja una planificación implícita y ejecución controlada del proceso de actualización.

El ciclo de supervisión (requerimiento → respuesta contratista → verificación supervisor, con cierre del ticket) ejemplifica la aprobación pero no corresponde al entregable establecido por el GIT TI en el Anexo.

De otro lado, por medio de los soportes documentales se identificó una reducción en el volumen de cambios de infraestructura a partir de enero de 2026 (de un promedio de 7,7 cambios/mes en el segundo semestre de 2025 a 1,8 cambios/mes en el primer semestre de 2026), y en junio-julio de 2026 (3–4 cambios/mes). Esta variación no constituye una situación de incumplimiento, pero se recomienda verificar que la reducción no sea atribuible a una disminución en la cobertura de actualizaciones, sino al ciclo natural de actividades del contrato y al estado de la infraestructura.

Frente a lo anterior, se identificó que el criterio, **CUMPLE PACIALMENTE**.

- III-4

Criterios: ISO/IEC 27001:2022

	INFORME DE SEGUIMIENTO Y EVALUACIÓN (Trabajos de informes, seguimientos de ley y/o cumplimiento)	CÓDIGO:	F-AU-10
		VERSIÓN:	04
		VIGENCIA:	2025-06-12
	AUDITORÍA INTERNA	CLASIFICACIÓN:	IP

A.5.37 – Documentación de procedimientos

A.8.32 – Cambios

Criterio de verificación (Anexo Técnico No. 2)

*“NETWORKING – Num. 3: El CONTRATISTA debe **realizar el estudio y análisis de los logs y alarmas** que arrojen los sistemas de administración y gestión de la seguridad. //*

ACTUALIZACIÓN (Num. 2): Deberá ejecutarse gradualmente de forma que se mantenga la compatibilidad y funcionalidad de los sistemas existentes.

En caso de que por razones de compatibilidad no se pueda realizar la migración o actualización, se deben implementar mecanismos de mitigación y salvaguardas para mantener la operación segura de los sistemas de la Entidad.”

Frente a este criterio, GTI indicó lo siguiente en su respuesta del 17 de septiembre de 2026:

“Por parte del operador para mitigar el riesgo de incompatibilidad toda la infraestructura de seguridad es de marca Fortinet con los siguientes componentes: SIEM: FortiSiem, NAC: FortiNac, DLP: FortiDLP, AntiSpam: Fortimail, para efecto de analisis de algunos logs la entidad cuenta con FortiAnalyzer. Se adjuntan informes SOC mensuales del periodo Solicitado.”

- Análisis por eje de criterio:

El análisis del criterio se realizó mediante la verificación de los Informes mensuales de Monitoreo SOC entregados por el GTI. para el período auditado, comprendido entre junio de 2025 y julio de 2026.

El análisis consideró:

- i) Verificación de continuidad en la entrega de informes SOC sin brechas de cobertura.
- ii) Confirmación de las secciones mínimas de análisis de logs y alarmas en cada informe.
- iii) Validación de la integración de dispositivos de seguridad Fortinet en el FortiSIEM para la correlación de eventos.
- iv) Revisión de la gestión de casos escalados (tickets), tendencias de amenazas y recomendaciones.
- v) Constatación del ecosistema tecnológico Fortinet declarado por el GTI, que garantiza la compatibilidad del monitoreo.

Frente al criterio, en los soportes documentales se indicó que, el GTI declaró que, con el propósito de mitigar el riesgo de incompatibilidad en la integración de herramientas de seguridad, toda la infraestructura de seguridad tecnológica de ENTerritorio S.A, opera bajo la marca Fortinet.

Los componentes integrados al SOC son los siguientes:

Componente	Producto Fortinet	Función en el monitoreo SOC
SIEM	FortiSIEM	Correlación de eventos, integración de dispositivos, gestión de loC, dashboards funcionales. Versión 7.4.2 activa al cierre del período.
NAC	FortiNAC	Control de acceso a la red, identificación y segmentación de dispositivos conectados.
DLP	FortiDLP	Prevención de pérdida de datos; monitoreo de exfiltración de información.

 Empresa Nacional Promotora del Desarrollo Territorial S.A.	INFORME DE SEGUIMIENTO Y EVALUACIÓN (Trabajos de informes, seguimientos de ley y/o cumplimiento)	CÓDIGO:	F-AU-10
		VERSIÓN:	04
		VIGENCIA:	2025-06-12
	AUDITORÍA INTERNA	CLASIFICACIÓN:	IP

Componente	Producto Fortinet	Función en el monitoreo SOC
AntiSpam / Email Security	FortiMail	Análisis de correo entrante/saliente, clasificación spam/phishing, reporte de virus, bloqueo de adjuntos maliciosos. Integrado desde Ago-Sep 2025.
Análisis de logs	FortiAnalyzer	Centralización y análisis de logs de toda la infraestructura de seguridad; correlación con eventos FortiSIEM.

El GTI, aportó un total de 13 Informes Mensuales de Monitoreo SOC que cubren ininterrumpidamente el período comprendido entre junio de 2025 y julio de 2026 (13 meses).

Los informes fueron elaborados por E&C Ingenieros (2H-2025, formato bimestral .DOC) y posteriormente por el contratista (a partir de diciembre 2025, formato mensual PDF con clasificación CONFIDENCIAL):

No.	Período cubierto	Emisión	Proveedor SOC	Págs.	Archivo de evidencia
1	Jun – Jul 2025	Jul 2025	E&C Ingenieros	N/D	INFORM2.DOC
2	Jul – Ago 2025	Ago 2025	E&C Ingenieros	N/D	INFORM1.DOC
3	Ago – Sep 2025	Sep 2025	E&C Ingenieros	N/D	IN2BDB1.DOC
4	Sep – Oct 2025	Oct 2025	E&C Ingenieros	52	IN24291.DOC
5	Oct – Nov 2025	Nov 2025	E&C Ingenieros	N/D	INFORM4.DOC
6	Nov – Dic 2025	Dic 2025	E&C Ingenieros	N/D	INFORM3.DOC
7	27 Dic 2025 – 26 Ene 2026	Ene 2026	UT ENTerritorio 2027	46	INFORME_SOC_ENTERRITORIO_ENERO_2026.pdf
8	27 Ene – 26 Feb 2026	Feb 2026	UT ENTerritorio 2027	46	INFORM3.PDF (Febrero 2026)
9	27 Feb – 26 Mar 2026	Mar 2026	UT ENTerritorio 2027	44	INFORME_SOC_ENTERRITORIO_MARZO_2026.pdf
10	27 Mar – 26 Abr 2026	Abr 2026	UT ENTerritorio 2027	56	INFORME_SOC_ENTERRITORIO_ABRIL_2026.pdf
11	27 Abr – 26 May 2026	May 2026	UT ENTerritorio 2027	63	INFORME_SOC_ENTERRITORIO_MAYO_2026.pdf
12	27 May – 26 Jun 2026	Jun 2026	UT ENTerritorio 2027	51	INFORME_SOC_ENTERRITORIO_JUNIO_2026.pdf
13	27 Jun – 26 Jul 2026	Jul 2026	UT ENTerritorio 2027	54	INFORME_SOC_ENTERRITORIO_JULIO_2026.pdf

 Empresa Nacional Promotora del Desarrollo Territorial S.A.	INFORME DE SEGUIMIENTO Y EVALUACIÓN (Trabajos de informes, seguimientos de ley y/o cumplimiento)	CÓDIGO:	F-AU-10
		VERSIÓN:	04
		VIGENCIA:	2025-06-12
	AUDITORÍA INTERNA	CLASIFICACIÓN:	IP

Frente a la estructura del análisis de logs y alarmas, se identificó que todos los informes SOC revisados contienen las siguientes secciones de análisis técnico, que dan evidencia del estudio sistemático de logs y alarmas de los sistemas de seguridad:

Sec.	Sección	Contenido / actividad de análisis
4.1	Escaneos sigilosos / Stealth Scans	Análisis de actividades de reconocimiento de red, identificación de IPs origen, bloqueo de firmas IPS
4.2	Ataques IPS / Ataques de red	Top 10 firmas IPS detectadas y bloqueadas; análisis de vectores de ataque más frecuentes
4.3	Malware / Botnet	IPs catalogadas como malware, top 10 firmas de malware, análisis de páginas consultadas con malware
4.4	Navegación web maliciosa	Top 10 páginas consultadas con malware; top 10 sitios maliciosos; usuarios con consultas maliciosas
4.5	Total eventos por severidad	Distribución de eventos por nivel de severidad (alta, media, baja, informativa) para el período
4.6	Alertas de alta prioridad	Detalle de casos escalados al equipo de seguridad con mayor impacto potencial
5.1	FortiRecon (Growdata, desde Ene 2026)	Inteligencia de amenazas externas: credenciales expuestas, certificados expuestos, CVEs detectadas en la huella digital de la entidad
5.2	FortiMail / Inteligencia de amenazas email	Categoría de correo, spam, virus, phishing, acción por fecha, top IPs clientes, actividad web
6	Gestión de eventos SOC	Tabla de casos escalados SOC, tickets abiertos/cerrados, estado de casos pendientes, tiempos de respuesta
7	Dispositivos Integrados FortiSIEM	Listado actualizado de dispositivos integrados; dashboards funcionales; versión del colector; IOC activados
9	Conclusiones	Análisis consolidado del comportamiento de la infraestructura; tendencias de amenazas; alertas de alto impacto
10	Recomendaciones	Acciones correctivas y preventivas propuestas al equipo de TI de ENTerritorio

Respecto a las principales Métricas de Monitoreo (2025), los informes del período E&C Ingenieros (junio – diciembre 2025) reportaron las siguientes métricas de actividad de monitoreo:

Período	Total eventos	Casos gestionados	Alertas alta prioridad	Aspectos relevantes
Jun–Jul 2025	452.379.191	51	15.539	USA principal origen ataques; 51 tickets gestionados
Jul–Ago 2025	N/D	49	347	Reducción 3,92% vs período anterior; 10 tickets pendientes
Ago–Sep 2025	1.381	43	N/D	Integración FortiMail; bloqueo IPs maliciosas
Sep–Oct 2025	N/D	N/D	N/D	Informe bimestral E&C (52 págs.)
Oct–Nov 2025	274.057.993	38	N/D	Integración FortiSIEM IoC; DNS.PTR.Records.Scan frecuente
Nov–Dic 2025	1.847.910	57	N/D	DNS.PTR.Records.Scan; ticket 44554 cerrado 27/11/2025 01:59

	INFORME DE SEGUIMIENTO Y EVALUACIÓN (Trabajos de informes, seguimientos de ley y/o cumplimiento)	CÓDIGO:	F-AU-10
		VERSIÓN:	04
		VIGENCIA:	2025-06-12
	AUDITORÍA INTERNA	CLASIFICACIÓN:	IP

El criterio III-4 exige que el contratista realice el estudio y análisis de los logs y alarmas que arrojen los sistemas de administración y gestión de la seguridad.

- Resultado de la verificación documental

Del análisis de las evidencias presentadas se concluye lo siguiente:

- i). Cobertura continua: Se constató la existencia de 13 informes SOC mensuales sin interrupciones, cubriendo ininterrumpidamente los 13 meses del período auditado (jun 2025 – jul 2026).
- ii) Análisis técnico evidenciado: Cada informe contiene secciones de análisis de escaneos sigilosos, ataques IPS, malware/botnet, navegación maliciosa, eventos por severidad y alertas de alta prioridad; es decir, cubre los principales vectores de amenaza que generan logs y alarmas en los sistemas de seguridad.
- iii) Integración FortiSIEM verificada: Los informes incluyen tablas de dispositivos integrados en el FortiSIEM, evidenciando la recopilación centralizada de logs. La versión FortiSIEM 7.5.1 se encontraba activa al cierre del período auditado.
- iv) Gestión de casos documentada: Cada informe contiene tabla de casos escalados SOC con identificador de ticket, fecha de apertura/cierre y estado, demostrando la trazabilidad de la respuesta a alarmas de alta prioridad.
- v) Compatibilidad tecnológica: La decisión del GTI de operar toda la infraestructura de seguridad bajo la marca Fortinet (FortiSIEM, FortiNAC, FortiDLP, FortiMail, FortiAnalyzer) elimina los riesgos de incompatibilidad en la integración de fuentes de logs y alarmas, dando cumplimiento a lo exigido por el Num. 2 complementario.

Dado lo anterior, se identificó que el criterio **CUMPLE**.

- III-5

Criterios: ISO/IEC 27001:2022

Cláusula 9.1 –Seguimiento y medición

Criterio de verificación (Anexo Técnico No. 2):

“DESCRIPCIÓN GENERAL ANEXO 2: Todas las características de seguridad solicitadas se deben ajustar a la familia de normas ISO27001, en especial ISO27001 e ISO27002 con las que cuenta la entidad. //

ANS – Num. 11: Los resultados del monitoreo son mantenidos por el contratista para que puedan ser consultados por ENTerritorio S.A, en cualquier momento durante el plazo de ejecución del contrato.

La información mantenida por el contratista le debe permitir a ENTerritorio S.A, verificar la disponibilidad histórica del servicio. [Obligación de segunda línea de supervisión GTI sobre cumplimiento contractual Anexo 2, conforme Manual M-PR-01 v2]”

En la respuesta dada el 17 de septiembre por GTI, se indicó lo siguiente:

“Aportamos ruta en el aplicativo Subversion (Tortoise) donde se dejan todos los informes de seguridad y de proceso administrativo de la ejecución del contrato en sus 8 líneas de servicio.”

	INFORME DE SEGUIMIENTO Y EVALUACIÓN (Trabajos de informes, seguimientos de ley y/o cumplimiento)	CÓDIGO:	F-AU-10
		VERSIÓN:	04
		VIGENCIA:	2025-06-12
	AUDITORÍA INTERNA	CLASIFICACIÓN:	IP

- Resultado de la verificación documental

Una vez verificados los soportes documentales, se identificó:

i). Mantenimiento de resultados: El repositorio Subversion en la URL declarada demuestra que el contratista mantiene un sistema estructurado y con control de versiones (Rev. 326) para la custodia de los resultados del monitoreo.

Las carpetas "Informes 2024/", "Informes 2025/" e "Informes 2026/" confirman la continuidad histórica desde el inicio del contrato.

ii) Consulta por ENTerritorio S.A en cualquier momento: La URL pública del repositorio (<https://www.enterritorio.gov.co/subversion/2024612/4.OPERACION/>) permite a la Sociedad acceder a los documentos del contrato a través del navegador web o cliente TortoiseSVN en cualquier momento durante el plazo de ejecución del contrato.

iii). Verificación de disponibilidad histórica: El sistema de control de versiones Subversion inherentemente mantiene el historial completo de todos los archivos cargados, permitiendo rastrear cambios, fechas de carga y revisiones anteriores. Esto cumple el requisito de que la información le permita a ENTerritorio S.A, verificar la disponibilidad histórica del servicio.

iv) Cobertura de las 8 líneas de servicio: Las 15 carpetas identificadas en el repositorio cubren tanto los informes técnicos de seguridad (SOC, pentesting, vulnerabilidades, BD) como la documentación administrativa y operativa del contrato, coherente con las líneas de servicio del Anexo Técnico No. 2.

Dado lo anterior, se identificó que el criterio **CUMPLE** respecto a lo indicado en el Anexo No. 2

Resultado general de verificación de los dominios 01, 04 y de las obligaciones de la supervisión:

No.	Descripción del criterio evaluado	Control / Marco normativo	Resultado
D01-1	Plantillas de hardening formalmente aprobadas por el supervisor del contrato	<i>ISO 27001:2022 A.8.9 – Gestión de la configuración</i>	CUMPLIMIENTO PARCIAL
D01-2	Gestión de vulnerabilidades técnicas (Nessus): detección, priorización y remediación	<i>ISO 27001:2022 A.8.8 – Gestión de vulnerabilidades técnicas</i>	CUMPLIMIENTO PARCIAL
D01-3	El CONTRATISTA deberá suministrar, a través de un tercero certificado para ello, el servicio de pentesting (prueba de intrusión controlada)	<i>ISO/IEC 27001:2022 A.8.8 – Gestión de vulnerabilidades técnicas A.8.29- Pruebas de seguridad en desarrollo y aceptación. Cubre las pruebas de seguridad sobre sistemas (incluye pruebas de</i>	CUMPLE

 Empresa Nacional Promotora del Desarrollo Territorial S.A.	INFORME DE SEGUIMIENTO Y EVALUACIÓN (Trabajos de informes, seguimientos de ley y/o cumplimiento)	CÓDIGO:	F-AU-10
		VERSIÓN:	04
		VIGENCIA:	2025-06-12
	AUDITORÍA INTERNA	CLASIFICACIÓN:	IP

No.	Descripción del criterio evaluado	Control / Marco normativo	Resultado
		<i>intrusión sobre aplicaciones y entornos)</i>	
D01-4	Pentesting anual por tercero independiente y certificado	ISO 27001:2022 A.8.8 / A.5.37	CUMPLIMIENTO PARCIAL
D01-5	Gestión de identidades: SSO y MFA para los sistemas de ENTerritorio S.A.	ISO 27001:2022 A.8.2 – Derechos de acceso privilegiado	CUMPLIMIENTO PARCIAL
D01-6	Seguridad IaaS CCP/CCA: gestión de vulnerabilidades en infraestructura propia	ISO 27001:2022 A.8.8 / A.8.9	CUMPLIMIENTO PARCIAL
D04-1	Fuentes integradas al SIEM FortiSIEM (mínimo 100 dispositivos / 1.000 EPS)	ISO 27001:2022 A.8.15 – Registro de eventos A.8.16 – Monitoreo	CUMPLE
D04-2	Reglas de correlación activas, personalizadas y parametrizadas en FortiSIEM	ISO 27001:2022 A.8.15 / A.8.16	CUMPLE
D04-3	Tablero de monitoreo de ciberseguridad en tiempo real (SOC/NOC)	ISO 27001:2022 A.8.15 / A.8.16	CUMPLE
D04-4	SOC 7x24x365 y gestión de incidentes en herramienta de ENTerritorio S.A.	ISO 27001:2022 A.8.16	CUMPLE
D04-5	Campos del ticket de incidente (criticidad, riesgo, alertas, respuesta) y ANS de Impacto Operativo	ISO 27001:2022 A.8.16	CUMPLIMIENTO PARCIAL
D04-6	Análisis forense digital conforme a A.5.24–A.5.28 ISO 27001:2022 (mín. 2/año)	ISO 27001:2022 A.5.24–A.5.28	N/A
D04-7	ANS de disponibilidad: 12 actas de conciliación mensuales y aplicación de penalidades	ISO 27001:2022 A.8.16	CUMPLE
III-1	Visitas de verificación a los Centros de Cómputo CCP y CCA	M-PR-01 v2 Ley 1474/2011	CUMPLE
III-2	Gestión de incidentes (P-RI-19) y aprobación de plantillas de hardening / plan de actualización	M-PR-01 v2 P-RI-19 v4	CUMPLE
III-3	Plan de actualización formal presentado y aprobado al inicio de cada vigencia contractual	ISO 27001:2022 A.5.37 – Procedimientos documentados	CUMPLIMIENTO PARCIAL
III-4	Estudio y análisis de logs y alarmas de los sistemas de seguridad (13 informes SOC)	ISO 27001:2022 A.5.37 / A.8.32	CUMPLE
III-5	Mantenimiento y acceso al repositorio de resultados del monitoreo (Subversion)	ISO 27001:2022 Cláusula 9.1 – Seguimiento y medición	CUMPLE

	INFORME DE SEGUIMIENTO Y EVALUACIÓN (Trabajos de informes, seguimientos de ley y/o cumplimiento)	CÓDIGO:	F-AU-10
		VERSIÓN:	04
		VIGENCIA:	2025-06-12
	AUDITORÍA INTERNA	CLASIFICACIÓN:	IP

Tal como se evidencia en la tabla anterior, de los 18 criterios evaluados en el Contrato No. 2024612 – Anexo Técnico No. 2, 10 obtuvieron resultado CUMPLE (56%), 7 presentaron CUMPLIMIENTO PARCIAL (39%) y 1 fue declarado No Aplica –N/A– (5,5%). Ningún criterio llegó a INCUMPLIMIENTO.

El comportamiento por dimensión, es el siguiente:

La Dimensión D01 – Controles de Seguridad Base es la de mayor concentración de brechas: 5 criterios de los 6 evaluados (D01-1, D01-2, D01-4, D01-5 y D01-6) resultaron en CUMPLIMIENTO PARCIAL.

De otro lado, la Dimensión D04 – SOC / SIEM / Monitoreo / Análisis Forense muestra el mejor desempeño relativo: de sus 7 criterios, 5 alcanzan CUMPLE (D04-1, D04-2, D04-3, D04-4 y D04-7), 1 presenta CUMPLIMIENTO PARCIAL (D04-5), 1 es N/A (D04-6 – análisis forense, servicio bajo demanda no activado ante 0 incidentes de criticidad relevante en el período). Esta dimensión acredita la solidez de la plataforma tecnológica de monitoreo en tiempo real.

En lo que corresponde al Seguimiento a las Obligaciones del Supervisor Contractual (GTI), 4 de los 5 criterios evaluados resultaron en CUMPLE (III-1, III-2, III-4 y III-5), evidenciando visitas de verificación efectuadas, activación apropiada de la gestión de eventos/incidentes, análisis de logs documentados en 13 informes SOC y repositorio Subversion activo. El único criterio con CUMPLIMIENTO PARCIAL (III-3) corresponde al plan de actualización de infraestructura: los 57 cambios se ejecutaron con cobertura del 100 % dentro del ANS mediante ARANDA ITSM, pero no se aportó el documento formal de planeación previo con aprobación escrita del supervisor al inicio de la vigencia.

En conjunto, el patrón identificado es el del Anexo No.2 Seguridad Tecnológica en sus dimensiones 01 y 04, con capacidad técnica y operativa instalada y en funcionamiento, cuyas brechas se concentran en la capa de formalización documental y en los mecanismos de reporte y aprobación formal por parte del supervisor, antes que en la ausencia de los servicios como tal.

Dado lo anterior, la Asesoría de Control Interno indica que, si bien no se generó estado de incumplimiento en ninguno de los 18 criterios analizados, y que GTI por medio de los soportes documentales dio a conocer la prestación continua y operativa de los servicios de seguridad tecnológica durante los 13 meses del período evaluado, es pertinente generar mejora continua en las obligaciones del supervisor y por ende, Asesoría de Control Interno formula la siguiente observación:

OBSERVACIÓN NÚMERO 1:

Debilidades en la formalización documental y en los mecanismos de aprobación y verificación del supervisor contractual (GTI) en la ejecución del Anexo Técnico No. 2 – Contrato No. 2024612: Dimensiones 01 y 04.

CRITERIO

El Manual de Supervisión e Interventoría de ENTerritorio S.A. y las cláusulas contractuales del Contrato No. 2024612 establecen que el Supervisor Contractual (GTI) debe ejercer un control formal, continuo y documentado sobre la ejecución de las obligaciones del contratista, lo que comprende:

	INFORME DE SEGUIMIENTO Y EVALUACIÓN (Trabajos de informes, seguimientos de ley y/o cumplimiento)	CÓDIGO:	F-AU-10
		VERSIÓN:	04
		VIGENCIA:	2025-06-12
	AUDITORÍA INTERNA	CLASIFICACIÓN:	IP

- i) La verificación periódica y formal de los entregables documentales estipulados en el Anexo Técnico No. 2;
- ii) La aprobación expresa y escrita de los planes, cambios e intervenciones de infraestructura previo a su ejecución; y
- iii) El registro en actas de seguimiento del estado de cumplimiento de cada obligación, con constancia de las observaciones de la supervisión y los compromisos del contratista. Igualmente, las buenas prácticas de gestión de seguridad tecnológica y los controles ISO 27001:2022 (A.8.8 y A.5.37) exigen que el ciclo de gestión de vulnerabilidades sea documentado, trazable y verificable por la supervisión con periodicidad mínima mensual.

CONDICIÓN

De los 18 criterios evaluados en el Contrato No. 2024612 – Anexo Técnico No. 2, 10 obtuvieron resultado CUMPLE (56%), 7 presentaron CUMPLIMIENTO PARCIAL (39%) y 1 fue declarado No Aplica –N/A– (5,5%). Ningún criterio llegó a INCUMPLIMIENTO. Los 7 que presentaron **CUMPLIMIENTO PARCIAL** (39%), se encuentran concentrados principalmente en la Dimensión D01 – Controles de Seguridad Base (5 de 6 criterios: D01-1, D01-2, D01-4, D01-5 y D01-6) y en el criterio **III-3** (plan de actualización de infraestructura).

Ningún criterio llegó a **INCUMPLIMIENTO**, y los servicios de seguridad tecnológica operaron de manera continua durante los 13 meses del período evaluado en el presente seguimiento.

Sin embargo, se verificó que las brechas identificadas no obedecen a la ausencia de los servicios contratados, sino a deficiencias en la **capa de formalización documental y de aprobación formal por parte del supervisor**, definidas en el detalle técnico del presente seguimiento indicado para los criterios: D01-1, D01-2, D01-4, D01-5, D01-6, D04-5 y III-3.

CAUSA

La situación descrita tiene origen en la **ausencia de instrumentos de gestión documental formalizados** que regulen el ejercicio de la supervisión contractual frente al Anexo Técnico No. 2 (dominios 01 y 04).

IMPACTO

La ausencia de los mecanismos de formalización descritos **debilita el ejercicio de la segunda línea de aseguramiento** por parte del GTI y genera los siguientes efectos:

- i) Los criterios con CUMPLIMIENTO PARCIAL no pueden ser elevados a cumplimiento pleno en la vigencia evaluada, aun cuando la prestación técnica del servicio fue continua y operativa durante los 13 meses del período,
- ii) La posición contractual de ENTerritorio S.A. frente a posibles reclamaciones o controversias con el contratista se ve limitada por la ausencia de aprobaciones escritas formales y de registros explícitos de verificación de entregables conforme a los controles establecidos por el mismo GTI en el Anexo No. 2 del contrato,
- (iii) La gestión de vulnerabilidades, si bien técnicamente ejecutada, carece de trazabilidad documental suficiente para acreditar ante organismos externos de control el cumplimiento del ciclo completo de remediación, y

	INFORME DE SEGUIMIENTO Y EVALUACIÓN (Trabajos de informes, seguimientos de ley y/o cumplimiento)	CÓDIGO:	F-AU-10
		VERSIÓN:	04
		VIGENCIA:	2025-06-12
	AUDITORÍA INTERNA	CLASIFICACIÓN:	IP

v) Se podría generar un riesgo de continuidad del patrón de cumplimiento parcial en el próximo período de evaluación si no se adoptan los correctivos de formalización requeridos. Lo anterior, sin que ello implique cuestionamiento a la calidad técnica de la operación de seguridad tecnológica prestada por el contratista durante el período evaluado.

RECOMENDACIONES:

1. Formalizar el catálogo de entregables documentales periódicos del contratista: Establecer, junto con el contratista, el catálogo mínimo de entregables documentales exigibles por período, con formatos definidos, contenidos mínimos obligatorios y fechas máximas de entrega que dé cuenta de la totalidad de los controles establecidos en el Anexo No. 2, por parte del GIT de Enterritorio S.A

2. Establecer un ciclo formal de seguimiento a la remediación de vulnerabilidades: Implementar y documentar un proceso de seguimiento al ciclo completo de gestión de vulnerabilidades (detección → priorización por criticidad CVSS → plan de remediación con plazos máximos aprobados → verificación de cierre → indicador de cobertura acumulada), con periodicidad mínima mensual. Los resultados deben reportarse explícitamente en las actas de seguimiento contractual y constituir un indicador de gestión verificable por la supervisión.

3. Fortalecer las actas de seguimiento como instrumento de verificación y aprobación formal: Incorporar en el orden del día de las actas de seguimiento contractual periódicas la verificación explícita de cada entregable del catálogo mínimo definido en la Recomendación 1, con registro del estado de cumplimiento, observaciones de la supervisión y compromisos del contratista con fechas de cierre. Esta práctica formalizará el ciclo supervisor → requerimiento → respuesta contratista → verificación supervisor que ya opera en la práctica mediante los tickets ARANDA, otorgándole eficacia. La implementación de las anteriores recomendaciones fortalecerá el ejercicio de la segunda línea de aseguramiento por parte del GTI, consolidará la posición contractual de ENTerritorio S.A. y permitirá elevar los criterios con cumplimiento parcial a cumplimiento pleno en el próximo ejercicio de evaluación, sin que ello implique un cuestionamiento a la calidad técnica de la operación de seguridad tecnológica prestada por el contratista durante el período evaluado.

CONCLUSIONES

La Asesoría de Control Interno, con base en la evaluación independiente de los 18 criterios evaluados correspondientes a las Dimensiones D01 – Controles de Seguridad Base, D04 – SOC/SIEM/Monitoreo/Análisis Forense, y las Obligaciones del Supervisor Contractual (GTI), para el período julio de 2025 a julio de 2026 del Contrato No. 2024612 (INA-007-2024) – Anexo Técnico No. 2 – Servicios de Seguridad Tecnológica, concluye lo siguiente:

- El GTI, soportó documentalmente la operación continua y funcional de la plataforma de ciberseguridad durante los 13 meses del período evaluado. La infraestructura tecnológica desplegada (FortiSIEM v7.5.1.0620 con 78 dispositivos integrados y 1.455 EPS en tiempo real, 123 reglas de correlación activas, operación SOC 7x24x365, 12 Actas de Conciliación ANS suscritas y un único descuento aplicado en el período (Acta 18, \$3.009.831,93), evidenció la prestación real y continua del servicio de seguridad tecnológica contratado. En ninguno de los 18 criterios analizados se configuró un estado de INCUMPLIMIENTO de los criterios priorizados del Anexo No. 2, para el presente seguimiento,

	INFORME DE SEGUIMIENTO Y EVALUACIÓN (Trabajos de informes, seguimientos de ley y/o cumplimiento)	CÓDIGO:	F-AU-10
		VERSIÓN:	04
		VIGENCIA:	2025-06-12
	AUDITORÍA INTERNA	CLASIFICACIÓN:	IP

- El patrón de observación identificado es uniforme y corresponde a que la brecha no se encuentra en la existencia o funcionamiento de los servicios, sino en la capa de formalización documental que debe acompañar su ejecución. Los 7 criterios con resultado CUMPLIMIENTO PARCIAL (D01-1, D01-2, D01-4, D01-5, D01-6, D04-5 e III-3) presentan, en todos los casos, la actividad técnica acreditada con ausencia o insuficiencia del documento formal que la soporte, apruebe o reporte con los contenidos mínimos exigidos por el Anexo Técnico No. 2 y por la norma ISO 27001:2022. Esta condición, aunque no constituye incumplimiento, genera riesgo jurídico, por lo que se efectuaron recomendaciones específicas por parte de la Asesoría de Control Interno, en la Observación Número 1.
- La Dimensión D04 muestra el desempeño más sólido, dado que, 5 criterios se encuentra en estado CUMPLE sobre 7 evaluados, lo que confirma la madurez operativa del Centro de Operaciones de Seguridad y la robustez del SIEM como eje central del servicio. La Dimensión D01, por el contrario, concentra la totalidad de las brechas documentales del contratista (5 de 6 criterios en CUMPLIMIENTO PARCIAL).
- El supervisor contractual del Anexo No. 2, cumple en 4 de sus 5 obligaciones verificadas (III-1, III-2, III-4 e III-5). La brecha identificada en III-3 (ausencia del plan formal de actualización con aprobación previa escrita) es de naturaleza análoga al patrón referido anteriormente: La actividad se ejecutó y los resultados son verificables en ARANDA ITSM (57 cambios, 100 % dentro del ANS), pero sin el instrumento de planeación formal previo que exige el Anexo No. 2, y la norma ISO 27001:2022 en su criterio A.5.37.
- En consecuencia, la Asesoría de Control Interno recomendó mecanismos de control, orientados a fortalecer la formalización documental, y las actas de seguimiento como instrumento de verificación y aprobación formal.
- La implementación de las recomendaciones formuladas permitirá a GTI elevar los criterios con cumplimiento parcial a cumplimiento pleno en el próximo ejercicio de seguimiento por parte de la Asesoría de Control Interno, consolidando la posición contractual de la Sociedad y la evidencia documentada de la segunda línea de aseguramiento, sin que lo anterior implique cuestionamiento a la calidad técnica de la operación de seguridad prestada durante el período evaluado.

Atentamente,

ORLANDO CORREA NÚÑEZ

Asesor con Funciones de Control Interno

Elaboró: **Luisa Fernanda Ríos Giraldo – contratista – Asesoría de Control Interno**