Al contestar por favor cite estos datos:
Radicado No.: 202518010001303

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

MEMORANDO

Bogotá D.C, 02-05-2025 14:03:48

PARA: ARMANDO VIVAS SALAMANCA
Gerente Grupo Tecnologías de la Información

BADIR ALBERTO ALI BADRAN
Gerente Grupo de Gestión de Riesgos

MONICA DUARTE ORTIZ
Subgerente de Operaciones y Administrativa

DE: ORLANDO CORREA NÚÑEZ
Asesor de Control Interno

ASUNTO: Se remite Informe definitivo auditoría MSPI 2024 y se solicita formulación del plan de mejoramiento

Cordial saludo para todos.

Teniendo en cuenta que el 25 de abril de 2025 a través del radicado 202518010001233 se notificó el informe preliminar con las observaciones evidenciadas/observadas durante la ejecución del trabajo de auditoría al Modelo de Seguridad y Privacidad de la Información MSPI y que únicamente se recibió respuesta de la Subgerencia de Operaciones en el plazo establecido (3 días hábiles), dando cumplimiento al Plan Anual de Auditorías vigencia 2025 se remite el informe final y se solicita la formulación del Plan de mejoramiento por parte de los responsables definidos en el cuadro que se relaciona a continuación, siendo el plazo máximo para remitir el Plan de mejoramiento el **14 de mayo de 2025**.

Observación	**Responsable de emitir respuesta**
Observación No. 1. Debilidades en la calidad y completitud de los activos de información	Grupo de riesgos
Observación No. 2: Debilidades en la implementación de controles internos para el reporte oportuno de novedades al Grupo de Tecnologías de la Información	Talento Humano y Subgerencia de Operaciones, Gerentes de Grupo y/o supervisores
Observación No. 3: Deficiencias en el seguimiento al programa integral de protección de datos personales	Grupo de riesgos
Observación 4: Debilidades en el Registro Documental de las Pruebas de Calidad de Software	Grupo Tecnologías de la información

Observación	Responsable de emitir respuesta
Observación 5: Debilidades en los controles sobre Cuentas Vinculadas a Operador Tecnológico Saliente	Grupo Tecnologías de la información
Observación 6. Debilidades en la gestión de copias de Seguridad y Transferencia de conocimiento en contratistas	Subgerencia de Operaciones, Tecnologías de la Información, Gestión de riesgos, Gerentes de Grupo y/o supervisores
Observación 7. Ausencia de Acuerdos de Confidencialidad en Servidores Públicos de Libre Nombramiento	Talento Humano
Observación 8. Deficiencias en la Implementación y Seguimiento de Controles de Seguridad Física	Servicios Administrativos
Observación 9. Deficiencias en la actualización y/o creación de guías de usuario	Grupo Tecnologías de la información

Quedamos atentos,

ORLANDO CORREA NUÑEZ
ASESOR DE CONTROL INTERNO

Proyectó: ANA JOSEFA CARRENO PEREZ - CONTRATISTA - ASESORIA DE CONTROL INTERNO
Elaboró: ANA JOSEFA CARRENO PEREZ - CONTRATISTA - ASESORIA DE CONTROL INTERNO
Adjuntos: F-AU-04_V03 Informe ejecutivo de auditoria - 25042025 - Definitivo.pdf(14), F-AU-19_V04 Observaciones de auditoria - 25042025.xlsx(12), F-AU-08_V05 Eficiencia y eficacia de controles Mspi.xls.xlsx(72)

enterritorio Empresa Nacional Promotora del Desarrollo Territorial S.A.	**INFORME EJECUTIVO DE AUDITORÍA**	CÓDIGO:	**F-AU-04**
		VERSIÓN:	**03**
		VIGENCIA:	**2024-05-28**
	AUDITORÍA INTERNA	CLASIFICACIÓN:	**IP**

Fecha (dd/mm/aa):	25/04/2025
Objeto de auditoría (aspecto evaluable):	Evaluar los controles y riesgos para el Modelo de Seguridad y Privacidad de la Información MSPI en ENTerritorio S.A. con base en la declaración de aplicabilidad versión 6, el instrumento de autodiagnóstico del MSPI de MinTIC y el manual de Seguridad de la Información vigente
Dependencia(s):	Gerencia General - Subgerencia Administrativa- Subgerencia de Operaciones
Proceso(s):	Gestión de riesgos, Gestión de las Tecnologías de la información, Gestión Administrativa, Gestión del talento humano y Gestión de proveedores
Objetivo (s) estratégico(s):	Perspectiva aprendizaje, objetivo de cumplimiento 3. Adelantar la sistematización integral de los procesos y servicios
Alcance:	**Control de cumplimiento:** Evaluación de 73 controles seleccionados de la declaración de aplicabilidad versión 6.0 del MSPI contra lo establecido en el formato de autoevaluación del MSPI MinTIc y el manual de Seguridad de la Información vigente. **Control de gestión y resultado**: Gestión de los responsables frente a la implementación de los controles seleccionados de la Declaración de Aplicabilidad versión 6.0 del MSPI.
Enfoque:	**Cualitativo:** Por la aplicación y monitoreo a los controles de seguridad de la información seleccionados de la declaración de aplicabilidad versión 6.0 del MSPI. **Cuantitativ**o: Nivel de implementación de los controles seleccionados para evaluar.
Objetivos:	1. Evaluar la implementación de los controles organizacionales seleccionados de la declaración de Aplicabilidad del MSPI 2. Evaluar la implementación de los controles personales seleccionados de la declaración de Aplicabilidad del MSP 3. Evaluar la implementación de los controles físicos seleccionados de la declaración de Aplicabilidad del MSPI 4. Evaluar la implementación de los controles Tecnológicos seleccionados de la declaración de Aplicabilidad del MSPI
Perfil de auditores:	*Ingeniero de sistemas: Ingeniero de sistemas y computación con experiencia en auditoría de sistemas de información y 5 años de experiencia en auditoría basada en riesgos. *Ingeniero de sistemas: Ingeniero de sistemas y computación con experiencia en auditoría de sistemas de información y 5 años de experiencia en auditoría basada en riesgos.
Período de análisis:	01 de enero de 2024 a 31 de diciembre de 2024
Muestra:	*Universo: 93 controles del MSPI de la declaración de aplicabilidad versión 6.0* *Muestra: 73 controles (29 administrativos, 8 personales, 13 físicos y 23 tecnológicos* *Controles no evaluados: 20 (8 administrativos, 1 físico y 11 tecnológicos)*

Riesgos y controles evaluados:	*Riesgos emergentes*: En el marco de la auditoría se identificaron dos riesgos emergentes relacionados con la gestión de activos de la información y seguimiento al programa integral de protección de datos personales ***Evaluación de riesgos y controles****:* De la matriz de riesgos SIAR, se evaluaron 15 riesgos y 33 controles para los cuales se estableció un promedio del 82 % de eficiencia en el diseño y en cuanto a la eficacia de la operación del 82% (27 efectivos de los 33 evaluados) A su vez, se identificaron 35 controles de la declaración de aplicabilidad, no asociados a los controles de la matriz SIAR con un promedio del 72% en el diseño y del 66% en la eficacia de la operación.
Metodología, procedimientos de auditoría e instrumentos a utilizar:	**Procedimientos de auditoría:** • Inspeccionar las evidencias de la ejecución de los controles de la declaración de aplicabilidad ,seleccionados para evaluar • Observación en sitio de la aplicación de los controles físicos • Observación en tiempo real mediante sesiones por Teams, de la aplicación de controles tecnológicos, organizacionales y personales (con los grupos de trabajo, operador tecnológico, oficial de seguridad de la información y profesionales de TI) • Realizar validaciones cruzadas al interior del equipo auditor con el fin de corroborar lo evidenciado. **Instrumentos:** • Formato Validación de controles seguridad de la información (papeles de trabajo) • F-AU-08 Efectividad controles, F-AU-21 Riesgos emergentes **Fuentes de información:** • Información suministrada por los lideres de SGSI, Gestión de riesgos, Tecnologías de la información, Servicios Administrativos, Subgerencia de operaciones, Talento humano, Administración del edificio • Operador Tecnológico contrato 2024612 • Sistema integral de administración de riesgos- SIAR • Sistema de gestión documental - ORFEO - LIRA • Plataforma SECOP II
Criterios técnicos de evaluación:	• NTC-ISO/IEC 27001:2022 • Resolución 500 de 2021 MINTIC • Resolución 746 de 2022 MINTIC • M-RI-06_V06 Manual de políticas de seguridad de la información • O-RI-01_V04 Política Institucional de Seguridad de la Información • P-RI-19 Gestión de incidentes en seguridad de la información • P-RI-23 Monitoreo a la gestión y al gobierno de la seguridad de la información institucional • P-TI-04 Desarrollo, Mantenimiento y Puesta en Producción de Software

	• IRI-01 INSTRUCTIVO IDENTIFICACIÓN Y CLASIFICACIÓN DE ACTIVOS DE INFORMACIÓN v.3 28/06/2024 • P-RI-22 Procedimiento Gestión de Datos Personales V. 4 28/06/2024

Conclusiones:

Fortalezas

- ENTerritorio hasta la fecha como buena práctica tiene tercerizados los servicios de administración, operación, mantenimiento, monitoreo y seguridad de la plataforma tecnológica con el operador tecnológico UT Enterritorio 2027, en el marco del contrato 2024612 (INA-007-2024), el cual es supervisado por el Grupo de Tecnologías de la información.

- En la vigencia 2024 se realizó el proceso de transición de la norma ISO 27001:2013 a la versión 2022 para alinear el sistema de gestión de seguridad de la información con las actualizaciones normativas y los desafíos emergentes del entorno tecnológico y de riesgos actuales

- Gestión de riesgos realiza sensibilizaciones periódicas a los servidores públicos y contratistas y emite piezas comunicacionales referente a la seguridad de la información.

Resultados de la evaluación

De los 73 controles evaluados, a través de las pruebas de auditoría por muestreo se establece que 55 se ejecutan como están diseñados y son efectivos, lo que representa el **75%**, los 18 restantes presentan oportunidades de mejora y/o tema por implementar, como se muestra a continuación:

TIPO DE CONTROL		EVALUADOS	IMPLEMENTADOS EFECTIVAMENTE	CON OBSERVACIONES	OBSERVACIONES
A5	CONTROLES ORGANIZACIONALES	29	21	8	*observación 1: A5.9 *observación 2: A.5.15 A.5.16 A.5.17 A.5.18 *observación 3: A.5.34 *observación 9 A.5.37 *observación 5: **A.5.16 A.5.18** *observación 6 :**A.5.11** *observación 8: A.5.2
A6	CONTROLES PERSONALES	8	5	3	*observación 7: A.6.2 A.6.6 *observación 6 :A.6.5
A7	CONTROLES FISICOS	13	11	2	*observación 8: A.7.4 A.7.8
A8	CONTROLES TECNOLOGICOS	23	19	4	*observación 2: A.8.2 - A.8.3 *observación 4:A.8.29 A.8.33

El detalle del análisis de los controles se presenta en el documento *F-AU-08_V05 Eficiencia y eficacia de controles Mspi.xls*

Se evaluó el diseño del 100% de los controles objeto de auditoría y para la evaluación de la efectividad se realizó por muestreo.

Controles A5. ORGANIZACIONALES

De los 29 controles evaluados se concluye la implementación efectiva de 20, que representa el 69 %, y se relacionan a continuación:

- Segregación de tareas
- Contacto con las autoridades
- Contacto con grupos de interés especial
- Seguridad de la información en la gestión de proyectos
- Uso aceptable de activos de información y otros asociados a la misma
- Clasificación de la información
- Etiquetado de la información
- Transferencia de la información
- Seguridad de la información en la relación con proveedores
- Requisitos de seguridad de la información en contratos con terceros
- Gestión de la seguridad de la información en la cadena de suministro de las TIC (Tecnologías de Información y Comunicación)
- Gestión del cambio, revisión y monitoreo de los servicios del proveedor o suministrador
- Planeamiento y preparación de la gestión de incidentes de seguridad de la información
- Evaluación y decisión en los eventos de seguridad de la información
- Respuesta a los incidentes de seguridad de la información
- Aprendizaje sobre los incidentes de seguridad de la información
- Recolección de evidencia
- Requisitos legales, estatutarios, regulatorios y contractuales
- Protección de registros
- Cumplimiento con las políticas, reglas y normas de la seguridad de la información

Los 9 restantes presentan oportunidades de mejora y/o tema por implementar en cuanto a:

- Calidad y completitud de los activos de información
- Implementación de controles internos para el reporte oportuno de novedades al Grupo de Tecnologías de la Información para gestionar los controles de acceso
- Seguimiento al programa integral de protección de datos personales
- Actualización, divulgación o creación de las guías o manuales de usuario de los aplicativos usados para la operación de los procesos
- Gestión de copias de Seguridad y Transferencia de conocimiento en contratistas de prestación de servicios profesionales

Controles A6. PERSONALES

De los 8 controles evaluados se concluye la implementación efectiva de 5 que representa el 63%, y se relacionan a continuación

- Revisión de antecedentes para funcionarios y contratistas
- Concientización, educación y entrenamiento en seguridad de la información
- Proceso disciplinario
- Trabajo remoto
- Reportes de eventos de seguridad de la información

Los 3 restantes refieren a la Ausencia de Acuerdos de Confidencialidad en Servidores Públicos de Libre Nombramiento y debilidades en la gestión de copias de Seguridad y Transferencia de conocimiento en contratistas

Controles A7. FISICOS

De los 13 controles evaluados se concluye la implementación efectiva de 11 que representa el 85%, y se relacionan a continuación:

- Entrada física
- Seguridad de oficinas, despachos e instalaciones
- Protección contra amenazas físicas y ambientales
- Trabajo en áreas seguras
- Escritorio y pantalla limpios
- Seguridad de activos fuera de las instalaciones
- Medios de almacenamiento
- Seguridad del cableado
- Mantenimiento de equipos
- Disposición o reutilización segura de equipos

Los 3 restantes presentan oportunidades de mejora y/o tema por implementar en cuanto a: sensibilización sobre controles físicos, debilidades en el control de registro de entrada y salida de computadores, y monitoreo a la seguridad física

Controles A8. TECNOLOGICOS

De los 23 controles evaluados se concluye la implementación efectiva de 19 que representa el 83%, y se relacionan a continuación:

- Dispositivos de punto final de usuario
- Acceso al código fuente
- Autenticación segura
- Gestión de la capacidad
- Gestión de vulnerabilidades técnicas
- Copia de seguridad de la información
- Registro
- Sincronización de reloj (clock)
- Seguridad en redes
- Seguridad de servicios de red
- Segregación de redes
- Uso de criptografía
- Desarrollo seguro del ciclo de vida
- Requerimientos de seguridad en aplicaciones
- Principios de arquitectura de sistemas e ingeniería seguras

	• Generación de código seguro • Desarrollo tercerizado • Separación de entornos de desarrollo, prueba y producción • Gestión de cambios Los 5 restantes presentan oportunidades de mejora y/o tema por implementar en cuanto a: • Registro documental de las pruebas de calidad de software, • Controles sobre cuentas de usuarios vinculadas a Operador Tecnológico Saliente, • La implementación de controles internos para el reporte oportuno de novedades al Grupo de Tecnologías de la Información sobre control de acceso a los servicios tecnológicos

Observaciones:	**Observación No. 1. Debilidades en la calidad y completitud de los activos de información**
	
	Se identificaron debilidades en la gestión y publicación de los activos de información correspondientes a la vigencia 2024, disponibles en la sección de transparencia de la página web de Enterritorio S.A. Las principales falencias son las siguientes:
	• De un total de 471 registros:
	  ○ 9 registros carecen de información o presentan errores de fórmula (#¡REF).
	  ○ 81 registros no incluyen datos esenciales, como el idioma, medio de conservación y/o soporte.
	• No se identificaron activos relacionados con hardware, lo que limita la categoría de activos reportados.
	• El formato publicado no se encuentra actualizado frente al que figura en el Gestor Documental, evidenciando una falta de consistencia en la gestión de documentos.
	• No se incluyó la publicación de los activos de información en la sección de datos abiertos, incumpliendo los principios de accesibilidad y transparencia.
	
	Criterios:
	
	I-RI-01 INSTRUCTIVO IDENTIFICACIÓN Y CLASIFICACIÓN DE ACTIVOS DE INFORMACIÓN v.3 28/06/2024. Numerales:
	5. CONDICIONES GENERALES -El inventario de activos debe ser realizado en cada uno de los procesos de ENTerritorio S.A. y la matriz de levantamiento de activos de información debe estar totalmente diligenciada sin espacios en blanco.
	7.1. IDENTIFICACION DE ACTIVOS DE INFORMACIÓN
	En esta etapa, se relacionan los diferentes Activos de Información que se identifican y que corresponden al proceso, como son:
	• 7.1.3 De Tipo Hardware, se relacionan todos los activos de información, correspondientes a equipos físicos informáticos y de comunicaciones como routers, servidores
	10. ELABORACIÓN Y PUBLICACIÓN DE LOS INSTRUMENTOS DE GESTIÓN DE LA INFORMACIÓN PÚBLICA.
	• Para elaborar el Registro de Activos de Información, se debe iniciar con el diligenciamiento del formato Encuesta de Levantamiento, Valoración y Calificación de Activos de Información de ENTerritorio S.A. F-RI-18, luego diligenciar el formato Registro de Activos de Información F-RI- 19,
	• Deben ser publicados en la página web de ENTerritorio S.A. y en el portal de Datos Abiertos del Estado Colombiano www.datos.gov.co.
	
	Control A5.9 Inventario de activos de información y otros asociados a la misma - declaración de aplicabilidad ISO 27001:2022

Observación No. 2: Debilidades en la implementación de controles internos para el reporte oportuno de novedades al Grupo de Tecnologías de la Información

Se identificaron fallas en los controles internos por parte de Talento Humano, los grupos de trabajo y/o supervisores, afectando el reporte oportuno de novedades al Grupo de Tecnologías. Estas deficiencias comprometen la gestión adecuada de los accesos de los funcionarios durante situaciones específicas, como se detalla a continuación:

- Vacaciones: De una muestra de 38 registros, se observó que 11 (29%) no cuentan con soporte de correo por parte de Talento Humano ni con registro en el sistema Aranda para la desactivación temporal de los usuarios correspondientes.

- Incapacidades y licencias: De una muestra de 24 registros, se identificó que 9 (38%) no fueron reportados a la Oficina de Tecnologías, lo que ocasionó la no desactivación de los usuarios durante los periodos correspondientes.

Contratistas
*Terminación anticipada: De una muestra de 10 registros se evidenció que 3 se reportaron a mesa de ayuda, 1 a través de correo electrónico y 2 a través de Teams, en estos últimos no se generó caso en Aranda. Para 7 registros no se evidenció notificación y para 6 registros se evidenció una diferencia entre 3 y 36 días de la fecha de desactivación del usuario en el Directorio Activo frente a la fecha de legalización de la terminación anticipada.

*Suspensiones: De una muestra de 10 registros revisados se evidenció que para el 100% de los casos no se notificó esta novedad para inactivar las credenciales de acceso durante estos periodos.

Criterios:
*CTROPERI-44: El Gerente de Grupo en el caso de contratistas y Grupo de Gestión del Talento Humano para los nuevos funcionarios por evento generan una solicitud a través del aplicativo ARANDA para los escenarios de ingreso, vacaciones, licencias, incapacidades, terminación de contrato, terminación anticipada o suspensión el cual es gestionado por la Mesa de Ayuda para la atención y validación de perfiles y roles con el Directorio Activo. En el caso de terminación de contrato se programan las fechas de vencimiento del contrato y automáticamente se desactiva el usuario a la media noche del día de la terminación del contrato. Adicionalmente, la mesa integral de servicios desactiva todo el licenciamiento que se le haya asignado en virtud del contrato que termina. Adicional, el Profesional de Seguridad de la Información y Datos Personales y Datos Personales semestralmente validará la información para la depuración y actualización de los roles de los usuarios de la entidad. Objetivo: Estandarizar los permisos de acceso a las aplicaciones y otorgarlos con base en los roles definidos, mantener actualizado los usuarios del directorio activo y evitar el acceso a los usuarios sin ningún vínculo contractual.

*Controles declaración de aplicabilidad A.5.15-16-17-18-A.8.2 - A.8.3 – ISO 27001:2022

Observación No. 3: Deficiencias en el seguimiento al programa integral de protección de datos personales

Se identificaron debilidades en los roles y responsabilidades asignados para el seguimiento del programa integral de protección de datos personales en ENTerritorio S.A. Durante la vigencia 2024, no se presentó al Comité Institucional de Gestión y Desempeño (CIGD) el estado del programa para

su revisión, lo que evidencia una falta de cumplimiento en los mecanismos establecidos para su supervisión y evaluación.

Criterios:

Procedimiento P-RI-22 Procedimiento Gestión de Datos Personales V. 4 28/06/2024 numeral 5. Roles y responsabilidades

b. Comité Institucional de Gestión y Desempeño: Este comité tendrá a su cargo las siguientes funciones específicas frente a la protección de datos personales:

• Revisar por lo menos dos veces al año el estado general del programa integral de protección de datos personales de ENTerritorio S.A.

Control declaración de aplicabilidad : A.5.34

Observación 4: **Debilidades en el Registro Documental de las Pruebas de Calidad de Software**

Durante la auditoría de los tres aplicativos desarrollados inhouse en la vigencia 2024, se identificaron deficiencias significativas en el registro documental de las pruebas de calidad de software, específicamente en el uso del formato F-TI-22 PRUEBAS DE CALIDAD DE SOFTWARE. Este no cumple integralmente con los requerimientos necesarios para determinar con precisión los resultados de las pruebas ejecutadas. A continuación, se detalla lo evidenciado:

- Caso 11550 Proceso Judiciales:
  - El primer atributo indica una prueba exitosa con un subatributo de indicador del 70%.
  - Sin embargo, el criterio de aceptación se marcó como "No Aprobado", generando inconsistencia en los resultados.
- Caso 17138 Tasación:
  - Los cinco atributos de la prueba fueron exitosos y el criterio de aceptación se calificó como "Aprobado".
  - No obstante, el formato no cuenta con la firma del profesional que realizó las pruebas, lo que afecta la validez del registro.
- Caso 16368 Liquidación de Contratos:
  - En el resumen de la prueba no se listan los atributos evaluados.
  - En la hoja “Atributos-SubAtr-Ítems” se evidencia que cuatro atributos fueron evaluados, de los cuales el primero arrojó un resultado de prueba no exitosa.

Además, se observó que no fueron aportados los manuales de usuario correspondientes para dos de los aplicativos evaluados (Tasación y procesos judiciales)

Estas deficiencias afectan la integridad y trazabilidad de un control en el proceso de desarrollo de software. La ausencia de registros completos y coherentes dificulta la identificación de problemas, el seguimiento de los criterios de aceptación y la validación de los resultados de las pruebas.

Criterios

Procedimiento P-TI-04 Desarrollo, Mantenimiento y Puesta en Producción de Software:

- *Actividad 9: Registrar pruebas de calidad de software.*
- *Actividad 10: Reasignar casos no aprobados para análisis y corrección.*
- *Actividad 18: Actualizar documentación afectada, incluyendo manuales de usuario y guías técnicas.*

Control declaración de aplicabilidad : A.8.29 - A.8.33

Observación 5: Debilidades en los controles sobre Cuentas Vinculadas a Operador Tecnológico Saliente

En la mesa de trabajo con el operador tecnológico, durante la verificación del control de segregación de funciones en los servidores de producción y de pruebas, se identificaron dos cuentas de usuario pertenecientes al operador tecnológico saliente. Asimismo, se detectaron dos usuarios administradores de capa media y servidores del operador actual, cuyo registro aún utiliza correos electrónicos asociados al operador saliente.

Aunque las dos primeras cuentas del operador saliente están desactivadas y no presentan un riesgo inmediato, persiste la posibilidad de que existan permisos residuales en sistemas vinculados, o que estas cuentas puedan ser reactivadas accidentalmente, comprometiendo la seguridad de la información. Por otro lado, los registros de los usuarios actuales con correos electrónicos del operador saliente representan una falta de estandarización que podría generar confusión y vulnerabilidades en la gestión de credenciales.

Criterios

- A.5.16 Gestión de identidades: La norma establece que las identidades digitales deben ser gestionadas adecuadamente. La falta de actualización de credenciales y correos electrónicos vinculados a operadores salientes señala una debilidad en este ámbito.
- A.5.18 Derechos de acceso: Este control aborda la asignación, revisión y revocación de derechos de acceso. La permanencia de permisos residuales en cuentas inactivas representa un incumplimiento de este criterio.

Observación 6. Debilidades en la gestión de copias de Seguridad y Transferencia de conocimiento en contratistas (compartido entre subgerencia de operaciones, Tecnologías de la Información, Gestión de riesgos)

En la verificación realizada con mesa de ayuda sobre el trámite de paz y salvo y la realización de copias de seguridad (backups) en una muestra de ocho contratistas, se evidenció lo siguiente: seis gestionaron el paz y salvo, tres solicitaron el respaldo de la información generada durante su relación contractual, y cuatro adjuntaron el paz y salvo a la última cuenta de cobro. Sin embargo, no se encontró evidencia de la ejecución consistente de copias de seguridad ni la implementación de un proceso formal de transferencia de información durante la relación contractual. Esta ausencia de respaldo documentado incrementa el riesgo de pérdida de información crítica, afecta la continuidad operativa y dificulta la transferencia de conocimiento al término del contrato. Además, esta situación genera vulnerabilidades relacionadas con la posible fuga de datos y la falta de disponibilidad de información.

Criterios:

A5.11. Devolución de los activos
A.6.5 Responsabilidades luego de la finalización o cambio de empleo

F-PR-05 ANEXO DE CONDICIONES GENERALES DEL CONTRATO DE PRESTACIÓN DE SERVICIOS PROFESIONALES Y/O APOYO A LA GESTIÓN
*EL CONTRATISTA dando cumplimiento a las políticas de protección de datos, información confidencial y privilegiada, deberá al momento del cumplimiento de la vigencia del contrato de prestación de servicios, observar el tratamiento de los datos, herramientas, actos, lineamientos,

medios físicos y digitales en los que se apoyó para el cumplimiento del objeto contractual suscrito y/o en los casos específicos retornar los materiales empleados. Así mismo, deberá realizar la gestión de archivo de los documentos en el sistema de gestión documental, el cierre de procesos en los sistemas de información y/o servicios de red que haya utilizado para el desempeño de sus actividades y la devolución de la información producida en el marco de su contrato. Esta entrega deberá realizarse al supervisor del contrato, previa aprobación de la Certificación de cumplimiento para el pago.

i) El CONTRATISTA deberá seguir el protocolo de Certificación de Entrega F-PR-23, por lo tanto, el Supervisor garantizará que se cumpla la cadena de custodia y el Protocolo de Gestión de Equipos y Material Devolutivo, verificando la devolución de los equipos y materiales facilitados por ENTerritorio S.A. de acuerdo con los objetos contractuales específicos que requieran elementos de información especiales para su cumplimiento, sin que por ello se desvirtúe la autonomía, intendencia técnica y administrativa con la que cuenta el CONTRATISTA.

Observación 7. Ausencia de Acuerdos de Confidencialidad en Servidores Públicos de Libre Nombramiento

Se identificó que los servidores públicos de libre nombramiento y remoción no cuentan con acuerdos de confidencialidad formalmente establecidos. Esta omisión representa un riesgo significativo para la protección de información sensible y estratégica de la organización, ya que no se garantiza que estos funcionarios mantengan el compromiso de resguardar la confidencialidad de los datos, tanto durante su relación laboral como después de su terminación.

La ausencia de dichos acuerdos incrementa la exposición a vulnerabilidades relacionadas con el uso indebido, divulgación no autorizada o fuga de información, comprometiendo la integridad, confidencialidad y disponibilidad de los procesos institucionales.

Criterios

CTROPERI-62 Cláusulas de confidencialidad de la información, datos personales y credenciales de acceso a los sistemas de información

Los Colaboradores al momento de legalización del contrato deben aceptar las cláusulas de confidencialidad de la información, datos personales y credenciales de acceso a los sistemas de información. El Profesional de Seguridad de la Información y Datos Personales y Datos Personales Por evento valida las cláusulas de confidencialidad de la información en los contratos. Objetivo: Evitar que los Colaboradores compartan información institucional, datos personales y credenciales de acceso a los sistemas de información con terceros no autorizados.

A.6.2. Términos y condiciones de empleo: Los acuerdos contractuales de empleo deben establecer las responsabilidades del personal y de la organización para la seguridad de la información.

A.6.6. Acuerdos de confidencialidad o no revelación: Los acuerdos de confidencialidad o no divulgación que reflejen las necesidades de la organización para la protección de la información deben ser identificados, documentados, revisados y firmados periódicamente por el personal y otras partes interesadas pertinentes.

Manual de seguridad de la información M-RI-06 versión 5

13.2.4 Acuerdos de confidencialidad o de no divulgación ENTerritorio S.A. cuenta con cláusulas de confidencialidad para los contratos con personas jurídicas y personas naturales. Dichas cláusulas

de confidencialidad tienen componente de seguridad de la información institucional y de los datos personales que se puedan conocer durante el vínculo contractual.

Observación 8. Deficiencias en la Implementación y Seguimiento de Controles de Seguridad Física

Se identificaron varias debilidades relacionadas con las responsabilidades definidas en el manual de seguridad de la información para servicios administrativos, que afectan la eficacia de los controles implementados:

1. **Ausencia de informes de monitoreo**:
   - Aunque se presentaron los informes de gestión mensuales en los inmuebles donde la UT Nova (2024920 (INA-047-2024) presta el servicio de vigilancia y seguridad privada, el área de Servicios Administrativos, encargada del seguimiento y evaluación de la funcionalidad de los controles de seguridad física, no emitió informes específicos que permitan evaluar su eficacia.
2. **Falta de sensibilización y capacitación**:
   - Durante la vigencia 2024, no se realizaron capacitaciones enfocadas en el buen uso y correcta aplicación de los controles de seguridad física.
     Esta omisión puede generar desconocimiento en el personal, afectando la efectividad de las medidas de seguridad.
3. **Deficiencias en el control de salida de equipos:**
   - En el edificio ubicado en la calle 26, se observó que el procedimiento de salida de equipos presenta una vulnerabilidad crítica.
     Aunque se solicita el serial del equipo, éste no es verificado ni contrastado para confirmar que pertenezca al usuario que registró el ingreso.
     Esta falencia permitió que el equipo auditor retirara equipos sin validación efectiva, exponiendo riesgos de pérdida o sustracción de bienes.

Criterios:
A.7.4 Monitoreo de la seguridad física
A.7.8 Emplazamiento y protección de equipos

Manual de seguridad de la información M-RI-06 versión 5

11.1.2 Controles de acceso físico
V. Se debe realizar sensibilización a los colaboradores sobre la seguridad física de las instalaciones por parte del grupo de servicios administrativos.
XII. Servicios Administrativos junto con Tecnologías de la información analizarán informes trimestrales sobre acceso al edificio y pisos de ENTerritorio S.A.

11.2 Seguridad de los equipos
Dar cumplimiento al procedimiento para la autorización y el registro del traslado de equipos tecnológicos fuera de la Entidad incluyendo otros lugares donde opere ENTerritorio S.A., siendo los grupos de Servicios Administrativos y Gestión de las Tecnologías de la Información las responsables de definir este procedimiento y otorgar las autorizaciones correspondientes, para ello quienes administren o ejerza supervisión de contratos que involucren equipos tecnológicos.

	Observación 9. Deficiencias en la actualización y/o creación de guías de usuario En el ejercicio auditor se identificaron debilidades en la documentación de los sistemas de información o aplicativos en uso, en cuanto a las guías o manuales de usuario disponibles en el enlace https://www.enterritorio.gov.co/subversion/guiasUsuario/, en donde se listan 123 documentos, con situaciones observadas como: guías con la anterior razón social (FONADE), versiones de hasta 8 años atrás, aplicativos no vigentes. En particular para el formato de vinculación de clientes-FVC (6 documentos según roles), Tiquetes (10 documentos según roles), inspektor (v. del 2016), GEOTEC para varios proyectos terminados, ZOOM aplicativo en desuso, entre otros. Si bien, se tiene este repositorio de guías de usuario por trazabilidad puede contener las guías de aplicativos en desuso o de aquellos que no han surtido cambios, no se observó otro mecanismo o repositorio que contenga las guías de usuario actualizadas para los aplicativos vigentes o en su versión actual, y su disponibilidad para los usuarios que requieran su consulta. Es de mencionar que se observó que los aplicativos como GRC y cuentas de cobro incluyen en su menú el manual de usuario, y fueron aportadas las guías de liquidaciones, y de LIRA, esta última en etapa de ajustes y verificaciones para su formalización. **Criterios**: A.5.37 Procedimientos operacionales documentados: Los procedimientos operativos de las instalaciones de procesamiento de la información se debe documentar y poner a disposición del personal que los necesite Manual de seguridad de la información M-RI-06 versión 5 12.1.1 Procedimientos de operación documentados: La documentación de todos los sistemas de información y servicios tecnológicos de ENTerritorio S.A. debe ser actualizada por los desarrolladores, cada vez que se efectúen cambios funcionales y/o técnicos en ellos
Causas	**Riesgo operativo**, explicado por las siguientes causas: **Observación1** • Errores de transcripción y/o fórmulas • Ausencia de puntos de control antes y después de la publicación de los activos de información **Observación2** • Ejecución parcial del control referente al reporte oportuno de novedades para gestionar las credenciales de acceso de funcionarios y contratistas. **Observación 3** • Priorizar la transición ISO 27001:2013 a 27001:2022 para recertificación • Falta de monitoreo a controles claves del procedimiento de Protección de datos personales **Observación 4** • Debilidad o ausencia de lineamientos claros para documentar los resultados de las pruebas • Falta de comunicación efectiva entre los equipos de desarrollo, pruebas y documentación puede dificultar el registro adecuado y completo de los procesos realizados • No contar con plataformas o herramientas que faciliten la documentación de las pruebas puede provocar registros dispersos o incompletos.

Recomendaciones	**Observación 5** • Debilidades en el proceso de transición relacionado con la gestión de cuentas del operador saliente y la revisión posterior. **Observación 6** • Falta de seguimiento a los requisitos para realizar copias de seguridad y transferir conocimiento durante y al finalizar los contratos • Falta de Supervisión y control • Delegar las actividades de copia de seguridad y transferencia de conocimiento exclusivamente en el contratista, sin contar con mecanismos para su verificación, puede provocar inconsistencias o incumplimientos. **Observación 7** • Cultura organizacional basada en la confianza y lealtad de los servidores • Ausencia de procedimientos formales para la firma de acuerdos de confidencialidad durante el ingreso de los servidores públicos de libre nombramiento y remoción **Observación 8** • Falta de seguimiento y monitoreo a los controles físicos **Observación 9** • En los cronogramas del proceso de desarrollo no se incluyen actividades y recursos para crear y/o actualizar documentación • Falta de estandarización para la organización documental de los sistemas de información **<u>Recomendaciones:</u>** • Actualizar el formato de activos de información y verificar la integridad de la información registrada antes de su aprobación y publicación (Grupo Gestión de riesgos) • Implementar acuerdos de confidencialidad para los servidores públicos vinculados en la modalidad de libre nombramiento y remoción al inicio de la relación laboral y su ratificación al término de esta (**Grupo Gestión de riesgos y Talento Humano**) • Reportar oportunamente todas las novedades que se presenten con funcionarios y contratistas al Grupo de tecnologías de la Información, a fin de restringir los controles de acceso y evitar posibles fugas de información (**Grupos Gestión del Talento Humano y Grupos de trabajo y/o supervisores)** • Actualizar la documentación para el Sistema de Gestión de Seguridad de la información publicada en el catálogo documental- micrositio SAR (**Grupo Gestión de riesgos**) • Incluir en el programa integral de protección de datos personales criterios o variables que permitan hacer seguimiento y generar insumos para la toma de decisiones por las instancias correspondientes (**Grupo de Gestión de riesgos**) • Ajustar el formato F-TI-22 pruebas de software, incorporando controles de validación automáticos en los campos obligatorios que permitan registrar información completa, como

atributos evaluados, criterios de aceptación y firmas requeridas **(Grupo Tecnologías de la información)**

- Incorporar en los cronogramas de desarrollo de software una actividad orientada en la creación y actualización de los manuales de usuarios y técnicos para cada aplicativo desarrollado o actualizado (**Grupo Tecnologías de la información**)

- Revisar periódicamente el cumplimiento del procedimiento P-TI-04_V05 *Desarrollo, mantenimiento y puesta en producción de software*, sus puntos de control y documentación, y realizar ajustes en tiempo real. (**Grupo Tecnologías de la información**)

- Revisar la eliminación completa de las cuentas asociadas al operador saliente, incluyendo la revocación de todos los permisos vinculados a sistemas y plataformas relacionadas, y actualizar el dominio del correo electrónico de los usuarios que continuaron con el operador actual (**Grupo Tecnologías de la Información**)

- Realizar capacitaciones a supervisores y contratistas, para que todos los involucrados comprendan sus responsabilidades sobre la gestión, uso del *OneDrive*, back up y entrega de información clave al finalizar la relación contractual (**Subgerencia de operaciones – Oficial de Seguridad de la Información**)

- Establecer un proceso formal para la generación y presentación de informes periódicos que evalúen la eficacia de los controles de seguridad física implementados. (**Servicios administrativos**)

- Realizar sensibilizaciones periódicas sobre la importancia y correcta aplicación de los controles de seguridad física (**Servicios Administrativos, oficial de seguridad de la información**)

- Incorporar herramientas tecnológicas que faciliten la verificación de seriales de equipos de cómputo y otros datos clave en los controles de seguridad (**Servicios Administrativos**)

- Incluir en la actualización del perfil de riesgos del proceso de tecnologías de la información, el análisis de riesgos e identificación de nuevos controles criptográficos, y plasmar en el acta el resultado del análisis realizado (**Grupos Gestión de riesgos y Tecnologías de la Información**)

- Asociar a la matriz SIAR los controles de la declaración de aplicabilidad que aún no tienen correlación con el fin de gestionar integralmente los riesgos de seguridad de la información (**Grupo de gestión de Riesgos**)

Elaboró:	
Auditores - Asesoría de Control Interno:	Ana Josefa Carreño Perez Celeny González Parra
Aprobó:	
Asesor de Control Interno:	Orlando Correa Núñez