20231200132243

Al contestar por favor cite estos datos:
Radicado No.: 20231200132243

Pública	X	**Pública Reservada**		**Pública Clasificada**	

MEMORANDO

Bogotá D.C, 17-11-2023

PARA: JUAN GUILLERMO ORTIZ JULIÁO
Subgerente Administrativo

BADIR ALBERTO ALI BALDRAN
Gerente de riesgos

ARMANDO VIVAS SALAMANCA
Gerente de Tecnologías de la Información

DE: Asesoría de Control Interno

ASUNTO: Informe de auditoría seguridad de la información (SGSI), plan de continuidad de negocio (PCN) y requisitos de accesibilidad en página web (NTC 5854)

Estimados Subgerente y Gerentes,

Una vez presentadas las observaciones formuladas por la Asesoría de Control Interno relacionadas con la auditoría de gestión cuyo objeto fue la: "*Evaluación del sistema de seguridad de la información - SGSI, del riesgo de ciberseguridad, del plan de continuidad de negocio (PCN) y la NTC 5854 de requisitos de accesibilidad en web",* envío el Informe Ejecutivo de Auditoría en pdf con el correspondiente soporte en Excel (formato de registro de observaciones y sus anexos).

Revisadas las argumentaciones presentadas al equipo auditor en la reunión de presentación de observaciones realizada por *Teams* el 14/11/2023 y los soportes allegados por el grupo de Tecnologías de la Información por correo electrónico en la misma fecha, los auditores

Calle 26 # 13-19, Bogotá D.C., Colombia. Tel: +57 (601) 915 6282
Línea de Transparencia: +57 01 8000 914 502
www.enterritorio.gov.co

encontraron procedente ajustar en su descripción la observación No.1, así como complementar las causas de la observación No. 5.

En el informe de auditoría (adjunto) se señalan los riesgos identificados y las recomendaciones establecidas por esta Asesoría, dando lugar a la formulación del plan de mejoramiento por parte de los responsables del proceso.

Con soporte en el informe adjunto se requiere que el plan de mejoramiento de esta auditoría de gestión sea formulado a más tardar el 01/12/2023 con plazo de ejecución de las acciones propuestas que no supere junio del 2024.

En caso de requerir apoyo metodológico de la Asesoría de Control Interno en la formulación de acciones para el plan, o en la revisión y retroalimentación de las acciones formuladas, para validar que las mismas resuelvan las causas de las problemáticas identificadas, este puede hacerse efectivo mediante reunión con los auditores designados.

Atentamente,

MIREYA LOPEZ CHAPARRO

Firmado digitalmente por MIREYA LOPEZ CHAPARRO
Fecha: 2023.11.17 15:44:05 -05'00'

Mireya López Ch.
Asesor de Control Interno

Copias: Paola Andrea Neira Duarte - Gerente Servicios Administrativos, Cecilia Inés Castro Murgas - Gerente Talento Humano, Maria Janeth Patiño - Gerente Senior Oficina Asesora Jurídica, Cesar Leonardo Monroy - Gerente Master TI, Yeison Yesid Rodríguez - Grupo de Comunicaciones, Nicolás Rey Gallego - Web Master, Jorge Luis Vargas - Oficial de Seguridad de la Información, Alvaro Abdala Arboleda - Oficial PCN, Carolina López Hernández - Profesional Servicios Administrativos.

Anexos: F-AU-04 Informe ejecutivo de auditoría, F-AU-19 registro de observaciones, F-AU-08 Efectividad de controles y F-AU-21 riegos emergentes

Elaboró: Adriana Ocampo - Contrato 2023561, Celeny Gonzalez - Contrato 2023563, Diego Alexis Ossa - Contrato 2023562.

Calle 26 # 13-19, Bogotá D.C., Colombia. Tel: +57 (601) 915 6282
Línea de Transparencia: +57 01 8000 914 502
www.enterritorio.gov.co

enterritorio Empresa Nacional Promotora del Desarrollo Territorial	**INFORME EJECUTIVO DE AUDITORÍA**	CÓDIGO:	**F-AU-04**
		VERSIÓN:	**02**
		VIGENCIA:	**2023-06-20**
	AUDITORÍA INTERNA	CLASIFICACIÓN:	**IP**

Fecha (dd/mm/aa):	17/11/2023
Objeto de auditoría (aspecto evaluable):	Evaluación del sistema de seguridad de la información, del riesgo de ciberseguridad, del plan de continuidad de negocio (PCN) y la NTC 5854 de requisitos de accesibilidad en web
Dependencia(s):	Gerencia General, Subgerencia Administrativa
Proceso(s):	Gestión de las Tecnologías de la información, Gestión de Riesgo, Gestión Administrativa, Gestión del talento humano
Objetivo (s) estratégico(s):	*Desempeño y gestión institucional*: Optimizar la gestión institucional fortaleciendo el modelo integrado de planeación y gestión al interior de la entidad, para lograr una adecuada gestión misional acompañada de las mejoras prácticas en la administración pública *Transparencia:* Ejecutar nuestra función pública con transparencia, garantizando el cumplimiento de metas y la satisfacción de clientes y ciudadanía en general
Alcance:	*Control de cumplimiento:* Por la evaluación de la normatividad y requisitos relacionados con la seguridad de la información, el plan de continuidad del negocio y la accesibilidad a la página web de Enterritorio. *Control de gestión y resultados:* Por la verificación de la gestión de seguridad de la información, de la estrategia del Plan de Continuidad del Negocio y de la accesibilidad a la página web de Enterritorio <u>Acceso a la información</u> El equipo auditor tuvo acceso a la información necesaria para lograr el alcance de la auditoría
Enfoque:	Cualitativo: Por la aplicación, seguimiento y monitoreo a las políticas de seguridad de la información, pruebas al plan de continuidad del negocio y accesibilidad a la página web de la Entidad Cuantitativo: Por la verificación del resultado de las pruebas del PCN, monitoreo del SGSI y calificación de la implementación de la NTC 5854
Objetivos:	1. Evaluar las políticas, componentes y controles de seguridad de la información y riesgos de ciberseguridad 2. Verificar la implementación de los componentes de la estrategia de continuidad del negocio 3. Evaluar la funcionalidad de los requisitos de accesibilidad de la página web de Enterritorio 4. Evaluar la materialización de riesgos y eficacia de los controles, identificar riesgos emergentes y analizar los factores de riesgos de fraude y corrupción en los procesos objeto de auditoría

Perfil de auditores:	• Ingeniera de sistemas con énfasis en software, especialista en Gerencia de Proyectos; experiencia en auditoría de más de 10 años y 5 en auditoría basada en riesgos. Certificada como auditor líder en HSEQ e ISO 27001 • Ingeniera de Sistemas, Especialista en auditoria de sistemas, experiencia en auditoría de más 7 años y 5 años de experiencia en auditoria basada en riesgos. Certificada en ISO 27001 • Ingeniero Industrial, especialista en ingeniería de la calidad y el comportamiento, magíster en gestión de organizaciones; con experiencia mayor a 10 años en auditoría, 6 años en auditoría basada en riesgos. Auditor integral HSEQ (ISO 9001:2015, ISO 14001:2015, ISO 45001:2018)
Período de análisis:	Enero a octubre de 2023
Muestra:	*Universo*: políticas y declaración de aplicabilidad de seguridad de la información, componentes del Plan de continuidad del negocio, y Accesibilidad de página web
Riesgos y controles evaluados:	Riesgos emergentes: En el marco de la auditoría se identificó un riesgo emergente relacionado con el incumplimiento de las políticas, inconsistencias en documentos, pruebas o actividades incompletas de la estrategia de plan de continuidad del negocio y seguridad de la información de la Entidad. *Evaluación de riesgos y controles:* Se evaluaron cinco riesgos y seis controles para los cuales se estableció un promedio de 76% en la eficiencia del diseño y del 75% de eficacia en la aplicación del control. Del mismo modo, en ejercicio de la auditoría se evaluó un riesgo del perfil de riesgos de corrupción vigente (**ROPETI-3** Publicación errada o adulteración de la información publicada en la página web) incluido en el anexo 6 de Función Pública.

RIESGO	CONTROL	EFICIENCIA DEL DISEÑO	EFICACIA DEL CONTROL
ROPERI-1: Incumplimiento de las disposiciones normativas o en la ejecución de actividades relacionadas con la administración de riesgos	CTROPERI-4: Informes de avance y/o gestión al cumplimiento de los sistemas de administración de riesgo	76%	70%
ROPERI-1: Incumplimiento de las disposiciones normativas o en la ejecución de actividades relacionadas con la administración de riesgos	CTROPERI-7: Análisis y revisión de normatividad sobre administración de riesgos	76%	60%
ROPERI-13: Debilidades en el monitoreo de los riesgos de la entidad	CTROPERI-4: Informes de avance y/o gestión al cumplimiento de los sistemas de administración de riesgo	76%	60%

Riesgos y controles evaluados:

ROPERI-4: Deficiencias en la definición e implementación de manuales, metodologías, procedimientos, informes u otros requisitos relacionados con la administración de riesgos	CTROPERI-7: Análisis y revisión de normatividad sobre administración de riesgos	76%	60%
ROPESI-5: Falta de articulación y seguimiento en el mantenimiento y mejora de los sistemas de gestión de la Entidad	CTROPERI-1: Planta eléctrica del edificio FONADE	76%	100%
ROPETH-19: Indisponibilidad del recurso humano	CTROPETH-14: Diseño, implementación y ejecución del plan de emergencias de la Entidad	76%	100%

Fuente: Elaboración propia basada en Matriz de riesgos y controles Enterritorio – SIAR 2023

Metodología, procedimientos de auditoría e instrumentos a utilizar:

Procedimientos de auditoría:

- Inspeccionar y rastrear documentalmente la ejecución de controles, pruebas, planes y estrategias
- Observar la ejecución de pruebas de la activación del Centro de Computo Alterno - CCA con retorno
- Consulta de apropiación de la estrategia y responsabilidades de los equipos del PCN
- Consulta de aplicación de políticas y controles con profesionales de TI, oficial de seguridad de la información y oficial de continuidad del del negocio
- Verificación de controles en tiempo real con operador tecnológico - 2021975 y profesionales de TI (vía Microsoft Teams)
- Validación accesibilidad página Web de Enterritorio en el Comprobador HTML: https://validator.w3.org/
- Inspección física mediante recorrido por los pisos de Enterritorio de la disposición de elementos de emergencia y planos de evacuación, y en el Centro de cómputo piso 28 del control de acceso, control de temperatura y humedad
- Realizar validaciones cruzadas de los hechos identificados

Instrumentos:

- F-RI-17 Declaración aplicabilidad (validación de controles seguridad de la información)
- PCN-EQUIPOS, PCN-PLANES, PCN-CCA (validación de componentes del PCN)
- Pruebas PCN (Resultados pruebas PCN)
- NTC 5854 (validación requisitos NTC 5854)
- F-AU-08 Efectividad controles, F-AU-21 Riesgos emergentes

Fuentes de información:

- Sistema integral de administración de riesgos- SIAR
- Sistema de gestión documental -ORFEO
- Plataforma SECOP II
- Información suministrada por los lideres de SGSI, PCN y Tecnologías de la información
- Operador tecnológico contrato 2021975

	• Lideres de equipos PCN, oficiales de seguridad de la Información y de continuidad del negocio
Criterios técnicos de evaluación:	• Ley 1712 de 2014 Ley de transparencia y acceso a la información • Ley 87 de 1993, "por la cual se establecen normas para el ejercicio del control interno en las entidades y organismos del estado y se dictan otras disposiciones" • Ley 1952 de 2019, "Por medio de la cual se expide el código general disciplinario se derogan la ley 734 de 2002 y algunas disposiciones de la ley 1474 de 2011 (…)" • Decreto único reglamentario 1078 de 2015, del sector de Tecnologías de Información y las Comunicaciones • Circular no. 09 de 2020 Contraloría General de la República, Plan de transición de acceso a fuentes de información de forma periódica a acceso en tiempo real. • Circular Externa 018 de 2021, Superintendencia Financiera de Colombia, capítulo XXXI sistema integral de administración de riesgos (SIAR) • Circular Externa No. 038 de 2009 de la Superintendencia Financiera de Colombia. • Guía para la administración del riesgo y el diseño de controles en entidades públicas, DAFP • G-RI-04 Guía metodológica de gestión de riesgos • NTC ISO/IEC 27001:2013 • NTC 5854 Accesibilidad a páginas Web • ISO 22301 Plan de Continuidad de Negocio • M-SI-01 Manual del Sistema Integrado de Gestión Enterritorio • M-RI-06 Manual de políticas de seguridad de la Información • M-RI-05 Manual de continuidad del Negocio • M-TI-01 Manual de Gestión de la Tecnología de la Información y las Comunicaciones • P-RI-17 Pruebas al PCN • P-RI-18 Mantenimiento y Revisión por la Dirección del Plan de Continuidad del Negocio • 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-RI-26 Verificación de aplicaciones y servicios de tecnologías de la información críticos instalados en el CCA
Conclusiones:	<u>Aspectos relevantes:</u> Enterritorio denota una adecuada gestión frente a la seguridad de la información e implementación de la estrategia de continuidad del negocio al tener documentados los lineamientos y políticas aplicables, sensibilización a nivel institucional y tercerizar la administración de la plataforma tecnológica y seguridad informática mediante contrato con operador tecnológico. Respecto de los requisitos de accesibilidad a la página web de la Entidad presenta un nivel de implementación del 94% frente a los requisitos de nivel A y AA según las directrices tecnológicas establecidas por la WCAG 2.1 (pautas de accesibilidad de contenido)

Conclusiones:	El oficial de continuidad del negocio estableció un mecanismo apropiado para organizar la documentación y soportes de ejecución del cronograma PCN, y actualización en el enlace SIAR de la intranet, facilitando su consulta. <u>Aporte a los objetivos estratégicos</u> La gestión de la seguridad de la información, de la continuidad del negocio e implementación de requisitos de accesibilidad web aporta al logro del pilar estratégico de *Desempeño y gestión Institucional* en la medida en que la Entidad protege los principios de confidencialidad, integridad y disponibilidad de la información institucional, y a su vez tiene implementada la estrategia de continuidad del negocio. Así mismo, el que la página WEB cumpla con estándares de accesibilidad aporta al pilar de *transparencia,* al facilitar el uso y el acercamiento de los ciudadanos y partes interesadas. <u>Políticas y componentes de seguridad de la información y riesgos de ciberseguridad</u> El contrato 2021975 con objeto “La prestación de servicios integrales en tecnologías de información y comunicaciones - TIC, para llevar a cabo la administración, operación, mantenimiento y la gestión tecnológica de las diferentes líneas de servicio de Enterritorio” (fecha inicio 26/01/2022 y fecha fin 26/11/2023) contiene 8 líneas de servicio en su alcance contractual para centro de cómputo principal - CCP, centro de cómputo alterno - CCA, centro de cómputo básico – CCB, calle 26 y sede de archivo central histórico - ACH, de las cuales principalmente tres en sus condiciones técnicas respaldan a la Entidad en la gestión de seguridad de la información, así: • Anexo No. 1 - Servicio especializado de infraestructura y centros de cómputo para ambientes productivos y de pruebas, nube publica, y servicios de administración, operación, soporte y mantenimiento. • Anexo No. 2 - Servicios de seguridad tecnológica: Servicio de implementación, administración y monitoreo de los controles se seguridad; Actualización, hardening, gestión de vulnerabilidades; SOC (Centro de Operaciones de Seguridad), certificados digitales, antimalware y antivirus, prevención de pérdida de datos (DLP), NAC (Network Access Control) y servicios de seguridad web-WAF • Anexo Técnico No. 5 – Servicios de movilidad integral Infraestructura de comunicaciones unificadas, Microsoft office 365, Telefonía IP, Terminales telefónica, OneDrive, SharePoint, TEAMS Lo anterior se verificó en sesiones virtuales con profesionales del operador tecnológico y profesionale4s de TI como se resume a continuación: • El SOC (Centro de Operaciones de Seguridad) es un servicio 7X24 lo que garantiza un monitoreo constante e integral a la infraestructura tecnológica, mediante la solución McAfee SIEM que recoge los *logs* de los diferentes componentes (firewall, antivirus, servidores, etc.) los correlaciona según casos de usos parametrizados y genera las alertas correspondientes con datos relevantes como IP origen, usuario y tipo de acción.

Conclusiones:	Estos resultados, así como los boletines de ciberseguridad emitidos por entidades competentes y eventos de seguridad materializados a nivel global, son insumos para adoptar o fortalecer los controles. • En el primer semestre 2023 se realizó el análisis de vulnerabilidades por parte del proveedor 2secure con la metodología *pentesting* (ataque simulado) con 13 ítems identificados: 7 de riesgo bajo, 5 de riesgo medio y uno de riesgo alto. Los ajustes aplicables fueron implementados por el grupo de TI y el Operador Tecnológico, en coordinación con el Oficial de seguridad de la información; en los casos de incompatibilidad por obsolescencia tecnológica de algunos componentes, se ejecutaron medidas alternas para atender las brechas identificadas. • En cuanto a seguridad del correo electrónico el office 365 cuenta con la configuración del SMTP (parametrización para correos salientes), de amenazas, reglas en 5 niveles, directivas de correos no deseados, *antiphising*, protección *antimalware*, tareas automáticas que generan avisos a los usuarios para su análisis y listado de remitentes de dominios confiables El cumplimiento del operador tecnológico en los aspectos mencionados es verificado por el supervisor del contrato (profesional TI) mediante los informes mensuales y anexos, actas de conciliación de ANS y servicios prestados por periodo. A nivel institucional la Entidad adoptó las políticas de seguridad en el manual M-RI-06 y *formato F-RI-17 la declaración da aplicabilidad* para los 14 dominios del anexo A de la ISO 27001:2013, sin presentar ninguna exclusión de controles. Una vez verificado dicho documento el equipo auditor concluye: • Los controles se gestionan adecuadamente, excepto cinco: A 8.1.1 Inventario de activos, A 9.2.1 Registro y cancelación del registro de usuarios, A 11.1.2 Controles de acceso físicos, A 13.2.2 Políticas y procedimientos de transferencia de información y A 18.1.4 Privacidad y protección de información de datos • Solo el 9% (10) describen en forma detallada el control o mecanismo de aplicación acorde con la documentación actual (ver observación No.2) En cuanto al procedimiento *P-RI-23 Monitoreo a la gestión y al gobierno de la seguridad de la información institucional*, sus actividades se cumplen en un 46% debido a que no recoge como insumo los soportes de controles aplicados por los diferentes grupos de trabajo, lo que evidencia que la Entidad no cuenta con un modelo integral de medición de las políticas adoptadas de SI. Para mitigar el impacto de los riesgos de ciberseguridad, la entidad suscribió la póliza de seguro de responsabilidad civil por pérdida de datos con vigencia del 20/04/2023 al 20/04/2024 *"con el fin de cubrir la responsabilidad de Enterritorio por el uso y tratamiento de información y la responsabilidad por la seguridad de los datos, cobertura riesgos cibernético: por datos personales, por datos corporativos, por empresas subcontratistas y por seguridad de los datos"* (INA-001-2023 CTO 2023557)

Conclusiones:

Componentes de la estrategia de continuidad del negocio

- Análisis de Impacto del Negocio - BIA (*Bussiness Impact Analysis*): publicado en la intranet - SIAR, aprobado el 2023/08/28 por el Comité Institucional de Gestión y Desempeño describe los aplicativos y servicios tecnológicos críticos, personal vital por proceso y RPO (*Recovery Time Objective o Tiempo Objetivo de Recuperación*) y RTO (*Recovery Point Objective o Punto Objetivo de Recuperación*) definidos por la Entidad
- Plan de recuperación de desastres informáticos - PRDI: tiene como objetivo definir la estrategia de replicación de los servicios de tecnología que soportan los procesos críticos de ENTERRITORIO según Análisis de impacto de Negocio BIA. Contiene 13 posibles escenarios y la estrategia aplicable para cada uno, no obstante, no se identifica la fecha de actualización o versión actual, y menciona documentos obsoletos como el GDI453 (*Plan de recuperación de desastres informáticos*) y PAP475 (*activación, comunicación y ejecución del plan de continuidad del negocio*)
- Equipos y responsabilidades: Los auditores en reunión con los líderes de cada equipo (de tecnología, de respuesta a emergencias, de apoyo administrativo, de coordinación y manejo de crisis – ECMC) verificaron el cumplimiento de las responsabilidades de la estrategia, denotando falta de apropiación frente al componente árbol de llamadas. El equipo de financiamiento ante contingencia de liquidez fue integrado a la estrategia en mayo de 2023 alineado con el procedimiento *P-FI-29 Financiamiento ante contingencia de liquidez;* sin embargo, a la fecha no hay pruebas ejecutadas de este componente.
- Centro de cómputo alterno - CCA: incluido en la línea de servicio No.1 del operador tecnológico (contrato 2021975), replica la información contenida en las bases de datos mediante la tecnología *Data Guard* entre el Centro de Datos de Enterritorio y el CCA, su funcionalidad es evaluada mediante las pruebas del cronograma anual del PCN.
- Centro Alterno de Operaciones - CAO: en la actualización del M-RI-05 manual de continuidad del negocio 2021/06/08 se elimina el CAO de la estrategia del PCN. Luego del (BIA) 2020, como primera alternativa se contempla el trabajo remoto; y como segunda, en el evento de requerir temporalmente de espacios físicos se puede acudir al arrendamiento de espacios "*Coworking*"; para ello el ECMC evaluará la situación y recursos necesarios durante la contingencia, y Servicios Administrativos incluyó en el presupuesto 2023 este rubro.
- Cronograma y plan de pruebas: El cronograma del PCN 2023 contiene 39 actividades de las cuales 38 (97%) a 30/10/2023 se encuentran cumplidas en plazos, pero 7 de estas presentan inconsistencias en los soportes de ejecución. El equipo auditor determinó que hace falta incluir en el plan anual del PCN actividades referentes a pruebas de recorrido y sorpresa, socialización / pruebas al componente de contingencia de liquidez, actualización periódica del PRDI, visitas de verificación al centro de cómputo del operador tecnológico, y articulación del ERP con la estrategia.
- Sensibilización y apropiación: En el marco de la semana del riesgo se socializó la estrategia PCN y sus componentes con los colaboradores que asistieron a la charla

Conclusiones:	24/10/2023 "*Charla virtual sobre gestión de ciberseguridad articulada con la continuidad del negocio*", así como actividades de capacitación incluidas en el cronograma anual alineado con el plan institucional de capacitación- PIC <u>Requisitos de accesibilidad de la página web de Enterritorio</u> La norma NTC 5854:2011 establece los requisitos de accesibilidad que se deben implementar en las páginas web bajo cuatro principios (Perceptible, Operable, Comprensible y Robusto) que se desarrollan en cumplimiento de los diferentes niveles de conformidad o "exigencia" A (37), AA (14) y AAA (22); de los cuales, el equipo auditor pudo determinar que en Enterritorio se cumplen los correspondientes a los niveles A y AA considerando que la norma toma como referencia las Pautas de Accesibilidad para el Contenido Web - **WCAG 2.0** (11/12/2008) del *The World Wide Web Consortium* (W3C) De este modo, frente a las Pautas de Accesibilidad al Contenido en la Web (*Web Content Accessibility Guidelines - WCAG*) establecidos en el Anexo 1 - Directrices de Accesibilidad Web de la Resolución 1519 del 2020 de MinTIC, Enterritorio se encuentra en un nivel de implementación del **94%** (47 de 50 ítems) según el informe **WCAG 2.1** (mayor nivel de exigencia). Con corte a septiembre 2023, de los tres ítems pendientes y en desarrollo, dos corresponden al nivel A (1.2.2 Subtítulos para el contenido de audio y 1.2.3 Audio descripción o una alternativa para medios basados en tiempo - AMBT de un medio grabado para material en video) y uno a AA (1.2.5 Audio descripción para todos los videos). Para la validación del cumplimiento de los lineamientos establecidos en la WCAG 2.1 se ingresó al "Comprobador HTML" https://validator.w3.org/, el cual permite realizar un diagnóstico en tiempo real y establece el estado de la página. Con su aplicación el equipo auditor pudo identificar para la página web de Enterritorio que arrojó cero errores (0), siete advertencias (7) y ciento veinticinco mensajes de Información (125), concluyendo que no se encuentran errores que generen incumplimiento, sino la oportunidad de realizar ajustes no funcionales o de acceso.
Observaciones:	**Observación No 1: Inadecuada aplicación de 5 controles asociados a las políticas de Seguridad de la Información** Para la vigencia 2023 cinco controles del Anexo A no demuestran adecuada aplicación con respecto a las políticas de Seguridad de la Información de la Entidad: Para la vigencia 2023 cinco controles del Anexo A no demuestran adecuada aplicación con respecto a las políticas de Seguridad de la Información de la Entidad: * A 8.1.1 Inventario de activos: no fue incluida la actualización del documento en la planeación de SI 2023, última actualización de Inventario de activos realizada en 2022 (publicado en febrero 2023). * A 9.2.1 Registro y cancelación del registro de usuarios: en reunión de verificación en tiempo real con el Operador Tecnológico (31/10/2023) se validó en el directorio activo - DA la fecha de bloqueo era 15/12/2023 para los usuarios aocampo, cgonzal1 y dossa, aun cuando los contratos iniciaron el 19/05/2023 y vencen el 03/01/2024, situación ajustada en

Observaciones:	soporte del 14/11/2023; lo evidenciado denota que, el DA no está sincronizado con la fecha de terminación de los contratos mediante un mecanismo o control automático permanente para todos los usuarios. * A 11.1.2 Controles de acceso físicos: Servicios Administrativos no generó de manera inmediata la solicitud (mediante correo electrónico) a la Administración del Edificio para la desactivación oportuna de las tarjetas de proximidad para 7 funcionarios retirados de mayo a septiembre de 2023. * A 13.2.2 Políticas y procedimientos de transferencia de información: a la fecha (8/11/2023) no se evidenció soporte que demuestre la suscripción entre Enterritorio y la DIARI de los documentos para la vigencia 2023: "Documento técnico de entendimiento CGR - ENTERRITORIO", y el Acuerdo de confidencialidad sobre la información transferida. * A18.1.4 Privacidad y protección de información de datos personales: según el procedimiento P-RI-22 Procedimiento Gestión de Datos Personales (6.4-actividad 1), los grupos de trabajo y el oficial de seguridad de la información no han realizado el análisis para identificar si en la necesidad de contratación y/o firma de convenios se requiere transmitir o transferir bases de datos con información personal a terceros, y emitir el concepto requerido para los contratos suscritos desde la adopción del procedimiento(2021-06-22) *Criterios:* 1. NTC ISO 27001:2013 Anexo A, Objetivos de control y controles de referencia 2. M-RI-06 Manual de políticas de seguridad de la información, 6.1.1 Objetivos, Roles, responsabilidades y autoridades en la seguridad de la información - Mantener los lineamientos de seguridad de la información actualizados, a efectos de asegurar su vigencia, nivel de eficacia y conformidad con las orientaciones estratégicas de la Entidad - 8.1.1 Inventario de Activos de Información III. El inventario de activos de información de la Entidad se debe actualizar anualmente teniendo en cuenta todos los cambios al contexto interno y los procesos misionales, estratégicos y de apoyo. 3. Circular no. 09 de 2020 CGR, Plan de transición de acceso a fuentes de información de forma periódica a acceso en tiempo real. **Observación No 2: Inconsistencias y errores en la Declaración de aplicabilidad adoptada por Enterritorio** La Declaración de aplicabilidad F-RI-17 (V.04, 26/01/2023) vigente y publicada en el catálogo documental Enterritorio registra inconsistencias y errores con respecto a controles de seguridad establecidos para el Anexo A de la norma ISO 27001, así: • 49% (56 de 114 controles) de los ítems se encuentran desactualizados en los códigos del control (columna E) en concordancia con la matriz de riesgos SIAR • 37,7% (43 de 114 controles) de los ítems no describen específicamente el control o mecanismo de aplicación concordante con las políticas establecida en el Manual de políticas de seguridad de la información M-RI-06 vigente (V.04, 2023-05-26) • 4% (4 de 114 controles) registran error en el código del procedimiento relacionado

Observaciones:	• 0,8% (1 de 114 controles) asigna erróneamente al Dominio - Control A7.2.3 Proceso disciplinario, los 5 controles del proceso de Auditoría Interna que no aplican para el proceso disciplinario. *Criterios:* 1. NTC ISO 27001:2013 - 6.1.3 Tratamiento de riesgos de la seguridad de la información: d) producir una declaración de aplicabilidad que contenga los controles necesarios (véanse el numeral 6.1.3 b) y c)) y la justificación de las inclusiones, ya sea que se implementen o no, y la justificación para las exclusiones de los controles del Anexo A. 2. Modelo de Seguridad y Privacidad de la Información. Identificación, Valoración Y Tratamiento de Riesgos. Guía N.8 Controles de Seguridad y Privacidad de la Información- 7. DECLARACIÓN DE APLICABILIDAD: La declaración de aplicabilidad debe indicar si los objetivos de control y los controles se encuentran implementados y en operación, los que se hayan descartado, de igual manera se debe justificar por qué algunas medidas han sido excluidas **Observación No. 3 Incumplimiento en el procedimiento de monitoreo de seguridad de la información** Para la vigencia 2023 el procedimiento P-RI-23 Monitoreo a la gestión y al gobierno de la seguridad de la información institucional no se aplica según lo establecido en la versión vigente numeral 6.1 REVISIÓN Y/O AJUSTES AL MODELO DE MEDICIÓN: actividades 1 y 2, porque no existen soportes del Modelo de medición de la seguridad de la información y F-DO-03 Plantilla memorando o correo electrónico de solicitud a los Grupo de trabajo; los numerales 6.2 APLICACIÓN DEL MODELO DE MEDICIÓN (actividades 4, 5 y 6) y 6.3 PRESENTACIÓN DE RESULTADOS (actividades 9 y 10) tampoco cuentan con soporte de su aplicación. *Criterio:* 1. P-RI-23 Monitoreo a la gestión y al gobierno de la seguridad de la información institucional capítulo 6. Desarrollo de actividades 2. G-RI-04 Guía metodológica de gestión de riesgos, 4.10 Monitoreo y seguimiento ("se hace necesario establecer o integrar procedimientos de monitoreo que permitan evaluar la efectividad de los Sistemas de Administración de Riesgo Operacional y detectar y corregir sus deficiencias o debilidades") 3. Guía para la administración del riesgo y el diseño de controles en entidades públicas, DAFP, 3.5 Monitoreo y revisión 5. Actividades de monitoreo: su propósito es desarrollar las actividades de supervisión continua (controles permanentes) en el día a día de las actividades, así como evaluaciones periódicas (autoevaluación, auditorías) que permiten valorar: (i) la efectividad del control interno de la entidad pública; (ii) la eficiencia, eficacia y efectividad de los procesos; (iii) el nivel de ejecución de los planes, programas y proyectos; (iv) los resultados de la gestión, con el propósito de detectar desviaciones, establecer tendencias, y generar recomendaciones para orientar las acciones de mejoramiento de la entidad pública. (…) *Continúa en siguiente página…*

Observaciones:	**Observación No.4 Desactualización del documento de árbol de llamadas** El documento de árbol de llamadas aportado por el Grupo de Gestión de Riesgos con fecha de actualización 26/04/2023 que hace parte de la estrategia de continuidad del negocio para la comunicación entre los equipos y personal vital ante un evento contingente, definida en el Manual de continuidad del negocio M-RI-05V.04; contiene 5 (de 67) colaboradores del personal vital que ya no laboraron o prestaron sus servicios en la Entidad (retirados entre julio de 2022 y marzo de 2023). Del mismo modo, 7 (de 57) integrantes de los equipos: Coordinación y Manejo de Crisis, Respuesta a Emergencias, Continuidad de los Procesos Críticos, Tecnología, organismos de apoyo externo y operador tecnológico no laboraron en la entidad (retirados entre abril 2022 a marzo de 2023). *Criterio:* M-RI-05 Manual de continuidad del negocio V.04, 11 Estructura del plan de continuidad del negocio - 11.5 Equipo de respuesta a emergencias; gestionar la actualización periódica del árbol de llamadas, respecto al listado de colaboradores de los diferentes equipos, así como de los centros de atención en salud cercanos a la Entidad o los de mayor utilización de los colaboradores, 11.4 Equipo de Tecnología Gestionar la actualización periódica del árbol de llamadas, respecto a los proveedores de servicios tecnológicos 11.6 Equipo de Apoyo Administrativo Gestionar la actualización periódica del árbol de llamadas en cuanto a los proveedores externos que prestan servicios de apoyo a la Entidad y a los procesos claves del negocio, así como de los organismos de apoyo externo. **Observación No 5 Actividades incompletas e inconsistencias en la ejecución de pruebas del plan PCN 2023** Para tres pruebas (E.2.1, E.2.2, E.2.3) no se diligenció el formato F-RI-13 preparación, ejecución y cierre de pruebas al plan de continuidad, para los ítems E1.2 Pruebas CCA sin retorno y E1.6 el formato F-RI-13 Prueba de Ciberseguridad registran fechas erradas de agosto y septiembre de 2022 siendo 2023; para los ítems A.2.1 y E.3.1 se usó formato obsoleto (F-TI-03) desde junio a octubre 2023 (actual F-RI-26 31/05/2023). No se tiene establecido el formato de evaluación de pruebas para medir la eficacia y eficiencia de las 9 pruebas ejecutadas. Así mismo, no se incluyeron en el cronograma del plan de continuidad 2023 ítems como: pruebas de recorrido y pruebas sorpresa, pruebas o actividades de divulgación de responsabilidades y articulación del componente Financiamiento ante contingencia de liquidez (integrado al manual de continuidad M-RI-05 en mayo del 2023), actualización del plan de recuperación de desastres informáticos - DRPI, integración del ERP, y visita de verificación de condición del servicio al Centro de Cómputo Principal del Operador Tecnológico (escalamiento superior). *Criterios:* 1. M-RI-05 Manual de Continuidad del negocio V.04 - 8.1.1 Políticas Generales; todo cambio relacionado con la legislación y que afecte la continuidad de negocio de ENTerritorio o que implique afectación sobre la operación debe ser documentado e implementado como parte integral del PCN - 15.2.1 Tipos de pruebas: escritorio, recorrido, componente, funcional, recorrido, simulacro, anunciada, sorpresa - 15.2.2.2 Ejecución de las pruebas Asegurar el diligenciamiento de los

Observaciones:	formatos diseñados para documentar la prueba, registrando el desarrollo de todas las actividades ejecutadas (tanto las que se consideraron en el diseño de la prueba como las que no) - 15.2.2.3 Cierre de las pruebas; finalizar y formalizar los formatos de documentación de las pruebas. Medir la eficacia y eficiencia de los programas de pruebas para las pruebas ejecutadas, utilizando el formato de evaluación de pruebas pactado. 2. P-RI-17 Pruebas al PCN, V.04 - 6.2 Planeación, ejecución y cierre de cada prueba, actividades 2,5,7 3. Circular Externa SFC 018 de 2021 - capítulo XXXI sistema integral de administración de riesgos (SIAR) - 4.3.1.3.2. Administración de la continuidad del negocio- a. Haber superado las pruebas necesarias para confirmar su eficacia y eficiencia - 5.3.3.Plan de contingencia de liquidez, i. Evaluación y proceso de pruebas sobre funcionamiento, en donde se prueben los aspectos estratégicos y operativos del plan, incluyendo los protocolos a seguir, la estrategia de comunicaciones, la operatividad de las líneas de liquidez disponibles y los roles y responsabilidades que deben ejercer cada uno de los funcionarios involucrados. 4. Plan de recuperación de desastres informáticos de Enterritorio - 6. Plan de pruebas - 6.1 Revisión posterior de la prueba - criterios de evaluación. **Observación No. 6 Extralimitación en la asignación de responsabilidades en un procedimiento** El procedimiento P-RI-23 Monitoreo a la gestión y al gobierno de la seguridad de la información institucional (V.03 2023/09/22) designa como responsable de la ejecución de actividades a la Asesoría de Control Interno así: • 5. CONDICIONES GENERALES: “Los planes de tratamiento deben ser documentados y formalizados en el formato de F-RI-05 Plan de manejo de Riesgos, y ser integrados al Sistema de Gestión de Riesgos en Seguridad de la Información y Continuidad del Negocio (SARSICN) y al Sistema de Gestión de Riesgo Operativo de la Entidad (SARO), por lo cual es responsabilidad de la Asesoría de Control Interno realizar el seguimiento a dichos planes.” • 6. DESARROLLO DE ACTIVIDADES Actividad 13: “Seguimiento a planes de tratamiento”. Extralimitando la asignación de responsabilidades de la actividad independiente de auditoría interna vía un procedimiento interno. *Criterios:* 1. Ley 87 de 1993, artículo 12, parágrafo: ""En ningún caso, podrá el asesor, coordinador, auditor interno o quien haga sus veces, participar en los procedimientos administrativos de la entidad a través de autorizaciones y refrendaciones"" 2. M-SI-01 MANUAL DEL SISTEMA INTEGRADO DE GESTIÓN v.5: numeral 3.4 Roles y responsabilidades de las líneas de defensa “Primera Línea de Defensa 1. La identificación de riesgos y el establecimiento de controles, así como su seguimiento, acorde con el diseño de dichos controles, evitando la materialización de los riesgos. Segunda Línea de Defensa su rol principal es asegurar que los controles y procesos de gestión del riesgo de la 1ª Línea de Defensa sean apropiados y funcionen correctamente" 3. Ley 1952 de 2019 código general disciplinario, capitulo II – Deberes, artículo 38. Deberes. Son deberes de todo servidor público, numeral 32. Adoptar el Sistema de Control Interno y la función

Observaciones:	independiente de Auditoría Interna de que trata la Ley 87 de 1993 y demás normas que la modifiquen o complementen.
Recomendaciones a partir de riesgos identificados:	**Riesgo operacional**, explicado por las siguientes causas: • Falta de fuentes directas de información y de información primaria confiable • Falta de controles automáticos. • Concentración de responsabilidades en la aplicación de controles. • Deficiente revisión y falta de seguimiento por parte del Oficial de Seguridad de la información en la aplicación de los controles y responsabilidades. • Falta de validación y socialización de documentos y controles con las áreas antes de su publicación • Falta de rigurosidad en el cumplimiento de las responsabilidades por parte de los equipos que componen la estrategia del PCN. • Falta de definición de los términos y frecuencia para la actualización del árbol de llamadas • Cambio de metodología en la medición del sistema de SI • Falta de estandarización de la metodología de preparación, ejecución y cierre de las pruebas, así mismo, en la cobertura de los componentes de la planeación y mantenimiento del PCN. **<u>Recomendaciones:</u>** • Revisar, gestionar la actualización y socializar la *Declaración de aplicabilidad (F-RI-17)* de acuerdo con la realidad operativa, normativa y documental de la Entidad. ***(Gestión de Riesgos – Oficial de Seguridad de la Información)*** • Implementar los correctivos para la adecuada aplicación de los cinco controles relacionados en la Observación No.1 ***(Gestión de Riesgos – Oficial de Seguridad de la Información, Oficina Asesora Jurídica, Servicios Administrativos, Tecnologías de Información)*** • Diseñar e implementar un modelo integral de evaluación de las políticas de SI y medir la madurez del sistema. ***(Gestión de Riesgos – Oficial de Seguridad de la Información)*** • Determinar la frecuencia de actualización y establecer lineamientos para que las áreas involucradas reporten las novedades sobre los contactos, proveedores y órganos externos como insumos para la actualización permanente y sistemática del árbol de llamadas. ***(Gestión de Riesgos – Oficial de Continuidad del Negocio, Talento Humano, Servicios Administrativos, Tecnologías de Información)*** • Incluir en el plan de PCN 2024 actividades enfocadas en la verificación de la estrategia del PCN del Operador tecnológico, integrar en la estrategia las condiciones acceso y funcionalidad del ERP, y los demás ítems referidos de pruebas y divulgación detalladas en la Observación No. 5. ***(Gestión de Riesgos – Oficial de Continuidad del Negocio)***

Recomendaciones a partir de riesgos identificados:	• Formalizar y aplicar un mecanismo para la evaluación integral de las pruebas ejecutadas del PCN y registrar su resultado ***(Gestión de Riesgos – Oficial de Continuidad del Negocio)*** • Modificar el procedimiento *P-RI-23 Monitoreo a la gestión y al gobierno de la seguridad de la información institucional* reasignando la actividad: Seguimiento a planes de tratamiento al responsable competente. ***(Gestión de Riesgos - Oficial de Seguridad de la Información, Planeación y Desarrollo Organizacional)*** • Gestionar la publicación de la documentación del SGSI vigente, en la intranet Enterritorio / Catálogo Documental Sistema de Administración de Riesgos – SIAR. ***(Gestión de Riesgos - Oficial de Seguridad de la Información, Grupo de Comunicaciones, Tecnologías de Información)***
Elaboró:	
Auditores - Asesoría de Control Interno:	Adriana María Ocampo - contrato 2023561 Celeny González Parra - contrato 2023563 Diego Alexis Ossa - contrato 2023562
Aprobó:	
Asesor de Control Interno:	Mireya López Ch.

	OBSERVACIONES DE AUDITORÍA	CÓDIGO:	F-AU-19
		VERSIÓN:	03
	AUDITORÍA INTERNA	VIGENCIA:	2023-06-20
		CLASIFICACIÓN	IP

Fecha (dd/mm/aa): 17/11/23

Objeto de auditoría: Evaluación del sistema de seguridad de la información, del riesgo de ciberseguridad, del plan de continuidad de negocio (PCN) y la NTC 5854 de requisitos de accesibilidad en web

Dependencia(s): Gerencia General, Subgerencia Administrativa

Proceso(s): Gestión de las Tecnologías de la información, Gestión de Riesgo, Gestión Administrativa, Gestión del Talento Humano, Gestión Jurídica

Registro y análisis de observaciones:

Descripción de la observación	Posibles Causa(s)	Riesgo(s) asociado(s):	Ocurrencia, repetición y/o frecuencia (calcular porcentaje)	Efectos (calcular o definir cualitativamente)	En cumplimiento del objetivo de auditoría (número)	Afecta el objetivo estratégico (Describirlo si aplica)	Responsable(s)- causas/ riesgos/ cumplimiento objetivo estratégico	Fecha de registro	Prueba o evidencia	Retroalimentación de la observación (responsables procesos)	Análisis de la ACI a partir de retroalimentación	Descripción inicial de la observación
Observación No 1: Inadecuada aplicación de 5 controles asociados a las políticas de Seguridad de la Información Para la vigencia 2023 cinco controles del Anexo A no demuestran adecuada aplicación con respecto a las políticas de Seguridad de la Información de la Entidad: * A 8.1.1 Inventario de activos: no fue incluida la actualización del documento en la planeación de SI 2023, última actualización de inventario de activos realizada en 2022 (publicado en febrero 2023). * A 9.2.1 Registro y cancelación del registro de usuarios: en reunión de verificación en tiempo real con el Operador Tecnológico (31/10/2023) se validó en el directorio activo - DA la fecha de bloqueo era 15/12/2023 para los usuarios aocampo, cgonzal1 y dossa, aun cuando los contratos iniciaron el 19/05/2023 y vencen el 03/01/2024, situación ajustada en soporte del 14/11/2023; lo evidenciado denota que, el DA no está sincronizado con la fecha de terminación de los contratos mediante un mecanismo o control automático permanente para todos los usuarios. * A 11.1.2 Controles de acceso físicos: Servicios Administrativos no generó de manera inmediata la solicitud (mediante correo electrónico) a la Administración del Edificio para la desactivación oportuna de las tarjetas de proximidad para 7 funcionarios retirados de mayo a septiembre de 2023. * A 13.2.2 Políticas y procedimientos de transferencia de información: a la fecha (8/11/2023) no se evidenció soporte que demuestre la suscripción entre Enterritorio y la DIARI de los documentos para la vigencia 2023: "Documento técnico de entendimiento CGR - ENTERRITORIO", y el Acuerdo de confidencialidad sobre la información transferida. * A18.1.4 Privacidad y protección de información de datos personales: según el procedimiento P-RI-22 Procedimiento Gestión de Datos Personales (6.4-actividad 1), los grupos de trabajo y el oficial de seguridad de la información no han realizado el análisis para identificar si en la necesidad de contratación y/o firma de convenios se requiere transmitir o transferir bases de datos con información personal a terceros, y emitir el concepto requerido para los contratos suscritos desde la adopción del procedimiento(2021-06-22) *Criterios:* 1. NTC ISO 27001:2013 Anexo A (Normativo), Objetivos de control y controles de referencia 2. M-RI-06 Manual de políticas de seguridad de la información, 6.1.1 Objetivos, Roles, responsabilidades y autoridades en la seguridad de la información - Mantener los lineamientos de seguridad de la información actualizados, a efectos de asegurar su vigencia, nivel de eficacia y conformidad con las orientaciones estratégicas de la Entidad - 8.1.1 Inventario de Activos de Información III. El inventario de activos de información de la Entidad se debe actualizar anualmente teniendo en cuenta todos los cambios al contexto interno y los procesos misionales, estratégicos y de apoyo.	1. Fuente primaria de la información no confiable 2. Deficiente revisión y seguimiento de aplicación del controles. 3. Concentración de responsabilidades en la aplicación de controles. 4. Falta de controles automáticos y fuentes directas de información.	ROPERI-1 Incumplimiento de las disposiciones normativas o en la ejecución de actividades relacionadas con la administración de riesgos. CTROPERI-4	4% (5 controles con deficiencias de los 114 del anexo A)	Posibles requerimientos por incumplimiento normativo Afectación de Confidencialidad, disponibilidad e integridad de la información	1 Evaluar las políticas y componentes de seguridad de la información y riesgos de ciberseguridad	1. Desempeño y gestión Institucional	Gestión de Riesgos - Oficial de seguridad de la Información Tecnología de la Información Servicios Administrativos	7/11/2023	1. hoja obs 1y2 FRI-17_Declarac aplicab 2. hoja obs1_controles SI 3. grabación reunión Microsoft Teams 03/11/2023 (Oficial de seguridad de la información) Correo electrónico De: <jvargas2@enterritorio.gov.co>, Enviado el lunes, 23 de octubre de 2023 7:32 p. m.	Mediante correo del martes 14/11/2023 (2:06 p.m.) el Gerente Master (cmonroy) Grupo de Tecnologías de la Información allegó documento: Reporte_Usuarios_ ENTerritorio.xlsx con listado de los usuarios contratados en el aplicativo ERP a corte del 14/11/2023 y existentes en el DA; información solicitada como parte de la presentación de los resultados para el ítem A 9.2.1 Registro y cancelación del registro de usuarios; indicando que *"la evidencia con la que se validó en el directorio activo la fecha de bloqueo del 15/12/2023 para los usuarios aocampo, cgonzal1 y dossa fue generada con el reporte del mes de mayo del año 2023 desde el aplicativo ERP para la activación de dichos usuarios"* Para los demás ítems A de esta observación no se recibió retroalimentación	Una vez analizado el nuevo soporte y los argumentos presentados en el correo por el grupo de TI para el ítem "A 9.2.1 Registro y cancelación del registro de usuarios", el equipo auditor concluye que la observación se mantiene, pero se ajusta con sustento en: 1. Si bien en el archivo recibido el 14/11/2023, posteriormente a la presentación de observaciones, (Reporte_Usuarios_ENTerritorio.xlsx), la fecha de caducidad es correcta 03/01/2024 para los usuarios: aocampo, cgonzal1 y dossa, la verificación se realizó en tiempo real en el DA el 31/10/2023 en reunión con operador tecnológico donde se evidenció fecha caducidad o bloqueo el 15/12/2023, lo que denota que esta fecha no esta sincronizada con la fecha real de terminación de los contratos, mediante un mecanismo o control automático permanente para todos los usuarios. Por otra parte al verificar el archivo mencionado se elimina lo referente a los otros dos casos registrados en la observación inicial como: se identifican 136 usuarios vencidos a mayo de 2023, e incluso dos personas con vencimiento al año 2031 (sin usuario de Enterritorio)	**Observación No 1: Inadecuada aplicación de 5 controles asociados a las políticas de Seguridad de la Información** Para la vigencia 2023 cinco controles del Anexo A no demuestran adecuada aplicación con respecto a las políticas de Seguridad de la Información de la Entidad: A 8.1.1 Inventario de activos: no fue incluida la actualización del documento en la planeación de SI 2023, última actualización de inventario de activos realizada en 2022 (publicado en febrero 2023). A9.2.1 Registro y cancelación del registro de usuarios: en reunión de verificación en tiempo real con el Operador Tecnológico (31/10/2023) se validó en el directorio activo - DA la fecha de bloqueo es 15/12/2023 para los usuarios aocampo, cgonzal1 y dossa, aún cuando los contratos vencen el 03/01/2024; del mismo modo, en documento soporte recibido como insumo para el DA se identifican 136 usuarios vencidos a mayo de 2023, e incluso dos personas con vencimiento al año 2031 (sin usuario de Enterritorio) A11.1.2 Controles de acceso físicos: Servicios Administrativos no generó de manera inmediata la solicitud (mediante correo electrónico) a la Administración del Edificio para la desactivación oportuna de las tarjetas de proximidad para 7 funcionarios retirados de mayo a septiembre de 2023. A 13.2.2 Políticas y procedimientos de transferencia de información: a la fecha (8/11/2023) no se evidenció soporte que demuestre la suscripción entre Enterritorio y la DIARI de los documentos para la vigencia 2023: "Documento técnico de entendimiento CGR - ENTERRITORIO", y el Acuerdo de confidencialidad sobre la información transferida. A18.1.4 Privacidad y protección de información de datos personales: según el procedimiento P-RI-22 Procedimiento Gestión de Datos Personales (6.4-actividad 1), los grupos de trabajo y el oficial de seguridad de la información no han realizado el análisis para identificar si en la necesidad de contratación y/o firma de convenios se requiere transmitir o transferir bases de datos con información personal a terceros, y emitir el concepto requerido para los contratos suscritos desde la adopción del procedimiento(2021-06-22)
Observación No 2: Inconsistencias y errores en la Declaración de aplicabilidad adoptada por Enterritorio La Declaración de aplicabilidad F-RI-17 (V.04, 26/01/2023) vigente y publicada en el catálogo documental Enterritorio registra inconsistencias y errores con respecto a controles de seguridad establecidos para el Anexo A de la norma ISO 27001, así: • 49% (56 de 114 controles) de los ítems se encuentran desactualizados en los códigos del control (columna E) en concordancia con la matriz de riesgos SIAR • 37,7% (43 de 114 controles) de los ítems no describen específicamente el control o mecanismo de aplicación concordante con las políticas establecida en el Manual de políticas de seguridad de la información M-RI-06 vigente (V.04, 2023-05-26) • 4% (4 de 114 controles) registran error en el código del procedimiento relacionado • 0,8% (1 de 114 controles) asigna erróneamente el dominio - Control A7.2.3 Proceso disciplinario, los 5 controles del proceso de Auditoría Interna que no aplican para el proceso disciplinario. *Criterios:* 1. NTC ISO 27001:2013 - 6.1.3 Tratamiento de riesgos de la seguridad de la información: d) producir una declaración de aplicabilidad que contenga los controles necesarios (véanse el numeral 6.1.3 b) y c)) y la justificación de las inclusiones, ya sea que se implementen o no, y la justificación para las exclusiones de los controles del Anexo A. 2. Modelo de Seguridad y Privacidad de la Información. 8.2 Fase de planificación, Identificación, Valoración y Tratamiento de Riesgos. 3. Guía N.8 Controles de Seguridad y Privacidad de la Información, 7. Declaración de aplicabilidad: La declaración de aplicabilidad debe indicar si los objetivos de control y los controles se encuentran implementados y en operación, los que se hayan descartado, de igual manera se debe	1.Falta de seguimiento por parte del Oficial de Seguridad de la información en la aplicación de los controles y responsabilidades. 2. Falta de validación en la aplicación de controles de las áreas correspondientes	ROPERI-1 Incumplimiento de las disposiciones normativas o en la ejecución de actividades relacionadas con la administración de riesgos. CTROPERI-7	91% (104 controles con inconsistencias o errores de 114 Controles de Seguridad)	Instrumento obsoleto y/o incompleto para el seguimiento y toma de decisiones de SI Baja efectividad de los controles de SI	1 Evaluar las políticas y componentes de seguridad de la información y riesgos de ciberseguridad	1. Desempeño y gestión Institucional	Gestión de Riesgos - Oficial de seguridad de la Información	20/10/2023	1. hoja obs 1y2 FRI-17_Declarac aplicab 2. F-RI-17 Declaración de aplicabilidad (V.04, 26/01/2023) 3.Matriz de riesgos SIAR		
Observación No. 3 Incumplimiento en el procedimiento de monitoreo de seguridad de la información Para la vigencia 2023 el procedimiento P-RI-23 Monitoreo a la gestión y al gobierno de la seguridad de la información institucional no se aplica según lo establecido en la versión vigente numeral 6.1 REVISIÓN Y/O AJUSTES AL MODELO DE MEDICIÓN: actividades 1 y 2, porque no existen soportes del Modelo de medición de la información y F-DO-03 Plantilla memorando o correo electrónico de solicitud a los Grupo de trabajo; los numerales 6.2 APLICACIÓN DEL MODELO DE MEDICIÓN (actividades 4, 5 y 6) y 6.3 PRESENTACIÓN DE RESULTADOS (actividades 9 y 10) tampoco cuentan con soporte de su aplicación. *Criterio:* 1. P-RI-23 Monitoreo a la gestión y al gobierno de la seguridad de la información institucional capítulo 6. Desarrollo de actividades 2. G-RI-04 Guía metodológica de gestión de riesgos, 4.10 Monitoreo y seguimiento ("se hace necesario establecer o integrar procedimientos de monitoreo que permitan evaluar la efectividad de los Sistemas de Administración de Riesgo Operacional y detectar y corregir sus deficiencias o debilidades") 3. Guía para la administración del riesgo y el diseño de controles en entidades públicas, DAFP, 3.5 Monitoreo y revisión 5. Actividades de monitoreo: su propósito es desarrollar las actividades de supervisión continua (controles permanentes) en el día a día de las actividades, así como evaluaciones periódicas (autoevaluación, auditorías) que permiten valorar: (i) la efectividad del control interno de la entidad pública; (ii) la eficiencia, eficacia y efectividad de los procesos; (iii) el nivel de ejecución de los planes, programas y proyectos; (iv) los resultados de la gestión, con el propósito de detectar desviaciones, establecer tendencias, y generar recomendaciones para orientar las acciones de mejoramiento de la entidad pública. (..)	1. Cambio de la metodología de la medición del sistema de SI. 2. Priorización de medición de los planes y no de las políticas de SI.	ROPERI-13 Debilidades en el monitoreo de los riesgos de la entidad. CTROPERI-4	54% (7 de 13 actividades del procedimiento no se están cumpliendo como está descrito).	Imposibilidad para medir e identificar desviaciones en la aplicación de las políticas de SI que orienten las acciones de mejoramiento	1 Evaluar las políticas y componentes de seguridad de la información y riesgos de ciberseguridad	1. Desempeño y gestión Institucional	Gestión de Riesgos - Oficial de seguridad de la Información	3/11/2023	Hojas: Obs 3 grabación reunión Microsoft Teams 03/11/2023 (Oficial de seguridad de la información) Correo electrónico De: <jvargas2@enterritorio.gov.co>, Enviado el lunes, 23 de octubre de 2023 7:32 p. m.		
Observación No.4 Desactualización del documento de árbol de llamadas El documento de árbol de llamadas aportado por el Grupo de Gestión de Riesgos con fecha de actualización 26/04/2023 que hace parte de la estrategia de continuidad del negocio para la comunicación entre los equipos y personal vital ante un evento contingente, definida en el Manual de continuidad del negocio M-RI-05V.04; contiene 5 (de 67) colaboradores del personal vital que ya no laboraron o prestaron sus servicios en la Entidad (retirados entre julio de 2022 y marzo de 2023). Del mismo modo, 7 (de 57) integrantes de los equipos: Coordinación y Manejo de Crisis, Respuesta a Emergencias, Continuidad de los Procesos Críticos, Tecnología, organismos de apoyo externo y operador tecnológico no laboraron en la entidad (retirados entre abril 2022 a marzo de 2023). *Criterio:* M-RI-05 Manual de continuidad del negocio V.04. 11 Estructura del plan de continuidad del negocio - 11.5 Equipo de respuesta a emergencias; gestionar la actualización periódica del árbol de llamadas, respecto al listado de colaboradores de los diferentes equipos, así como de los centros de atención en salud cercanos a la Entidad o los de mayor utilización de los colaboradores, 11.4 Equipo de Tecnología Gestionar la actualización periódica del árbol de llamadas, respecto a los proveedores de servicios tecnológicos 11.6 Equipo de Apoyo Administrativo Gestionar la actualización periódica del árbol de llamadas en cuanto a los proveedores externos que prestan servicios de apoyo a la Entidad y a los procesos claves del negocio, así como de los organismos de apoyo externo.	1. Falta de rigurosidad en el cumplimiento de las responsabilidades por parte de los equipos que componen la estrategia. 2. Falta de definición de los términos y frecuencia para la actualización de este documento (en consideración que debería actualizarse cada vez que cambie un miembro del equipo por ser contactos de emergencia)	ROPERI-4 Deficiencias en la definición e implementación de manuales, metodologías, procedimientos, informes u otros requisitos relacionados con la administración de riesgos CTROPERI-7	7% (5 de 67 contactos del personal vital están desactualizados) 12% (7 de 57 integrantes de los contactos que componen los equipos y apoyo externo están desactualizados)	Incremento en el Tiempo Objetivo de Recuperación (RTO) de activación	2)Verificar la implementación de los componentes de la estrategia de continuidad del negocio	1. Desempeño y gestión Institucional	Gestión de Riesgos Gestión del Talento Humano Servicios Administrativos Tecnologías de la Información	25/10/2023	Hojas: Obs 4. A-llamadas-EQ y PV Relación de funcionarios, colaboradores y proveedores que no se encuentran en la Entidad y están incluidos en el documento árbol de llamadas. Cronograma PCN 2023, ítem A.1.9. Actualizar árbol de llamadas Obs 4y5_Pruebas PCN (columna K)		
Observación No 5 Actividades incompletas e inconsistencias en la ejecución de pruebas del plan PCN 2023 Para tres pruebas (E.2.1, E.2.2, E.2.3) no se diligenció el formato F-RI-13 preparación, ejecución y cierre de pruebas al plan de continuidad, para los ítems E1.2 Pruebas CCA sin retorno y E1.6 el formato F-RI-13 Prueba de Ciberseguridad registran fechas erradas de agosto y septiembre de 2022 siendo 2023; para los ítems A.2.1 y E.3.1 se usó formato obsoleto (F-TI-03) desde junio a octubre 2023 (actual F-RI-26 31/05/2023). No se tiene establecido el formato de evaluación de pruebas para medir la eficacia y eficiencia de las 9 pruebas ejecutadas. Así mismo, no se incluyeron en el cronograma del plan de continuidad 2023 ítems como: pruebas de recorrido y pruebas sorpresa, pruebas o actividades de divulgación de responsabilidades y articulación del componente Financiamiento ante contingencia de liquidez (integrado al manual de continuidad M-RI-05 en mayo del 2023), actualización del plan de recuperación de desastres informáticos - DRPI, integración del ERP, y visita de verificación de condición del servicio al Centro de Cómputo Principal del Operador Tecnológico (escalamiento superior). *Criterios:* 1. M-RI-05 Manual de Continuidad del negocio V.04 - 8.1.1 Políticas Generales; todo cambio relacionado con la legislación y que afecte la continuidad de negocio de ENTerritorio o que implique alteración sobre la operación debe ser documentado e implementado como parte integral del PCN - 15. Planes asociados al PCN, 15.2.1 Tipos de pruebas: escritorio, recorrido, componente, funcional, recorrido, simulacro, anunciada, sorpresa - 15.2.2 Ejecución de las pruebas Asegurar el diligenciamiento de los formatos diseñados para documentar la prueba, registrando el desarrollo de todas las actividades ejecutadas (tanto las que se consideraron en el diseño de la prueba como las que no) - 15.2.2.3 Cierre de las pruebas; finalizar y formalizar los formatos de documentación de las pruebas. Medir la eficacia y eficiencia de los programas de pruebas para las pruebas ejecutadas, utilizando el formato de evaluación de pruebas pactado. 2. P-RI-17 Pruebas al PCN, V.04 - 6.2 Planeación, ejecución y cierre de cada prueba, actividades 2,5,7 3. Circular Externa SFC 018 de 2021 - capítulo XXXI sistema integral de administración de riesgos (SIAR) - 4.3.1.3.2. Administración de la continuidad del negocio- a. Haber superado las pruebas necesarias para confirmar su eficacia y eficiencia - 5.3.3.Plan de contingencia de liquidez, i. Evaluación y proceso de pruebas sobre funcionamiento, en donde se prueben los aspectos estratégicos y operativos del plan, incluyendo los protocolos a seguir, la estrategia de comunicaciones, la operatividad de las líneas de liquidez disponibles y los roles y responsabilidades que deben ejercer cada uno de los funcionarios involucrados. 4. Plan de recuperación de desastres informáticos de Enterritorio - 6. Plan de pruebas - 6.1 Revisión posterior de la prueba - criterios de	1. Falta de estandarización de la metodología de preparación, ejecución y cierre de las pruebas 2. Falta de cobertura de todos los componentes en la planeación y mantenimiento del PCN. 3. Falta de validación de los campos en los formatos diligenciados y en la impresión digital del documento	Emergente 1 Incumplimiento de las políticas, inconsistencias en documentos, pruebas o actividades incompletas de la estrategia de plan de continuidad del negocio y/o seguridad de la información de la Entidad	18% (7 actividades de las 39 que componen el cronograma 2023)	Insumos insuficientes para el plan de mantenimiento de la estrategia Subregistro de eventos que pueden afectar la continuidad del negocio	2)Verificar la implementación de los componentes de la estrategia de continuidad del negocio	1. Desempeño y gestión Institucional	Gestión de Riesgos - Oficial de Continuidad del Negocio	7/11/2023	Hojas: 1. Obs 4y5_Pruebas PCN (columna K) 2. Hoja Obs 5 3. carpeta compartida : Soportes Actividades PCN - Corte agosto 2023 (De: <sarboledi@enterritorio.gov.co> Enviado el: martes, 7 de noviembre de 2023 10:26 a. m.		En reunión de presentación de observaciones del 14/11/2023 se incluyó la causa N.3 aportada por los auditados
Observación No. 6 Extralimitación en la asignación de responsabilidades en un procedimiento El procedimiento P-RI-23 Monitoreo a la gestión y al gobierno de la seguridad de la información institucional (V.03 2023/09/22) designa como responsable de la ejecución de actividades a la Asesoría de Control Interno así: • 5. CONDICIONES GENERALES : "Los planes de tratamiento deben ser documentados y formalizados en el formato de F-RI-05 Plan de manejo de Riesgos, y ser integrados al Sistema de Gestión de Riesgos en Seguridad de la Información y Continuidad del Negocio (SARSCN) y al Sistema de Gestión de Riesgo Operativo de la Entidad (SARO), por lo cual es responsabilidad de la Asesoría de Control Interno realizar el seguimiento a dichos planes." • 6. DESARROLLO DE ACTIVIDADES Actividad 13: "Seguimiento a planes de tratamiento". Extralimitando la asignación de responsabilidades de la actividad independiente de auditoría interna vía un procedimiento interno. *Criterios:* 1. Ley 87 de 1993,artículo 12 Funciones de los auditores internos, parágrafo: "En ningún caso, podrá el asesor, coordinador, auditor interno o quien haga sus veces, participar en los procedimientos administrativos de la entidad a través de autorizaciones y refrendaciones" 2. M-SI-01 Manual del Sistema Integrado de Gestión v.5, numeral 3.4 Roles y responsabilidades de las líneas de defensa "Primera Línea de Defensa 1. La identificación de riesgos y el establecimiento de controles, así como su seguimiento, acorde con el diseño de dichos controles, evitando la materialización de los riesgos. Segunda Línea de Defensa su rol principal es asegurar que los controles y procesos de gestión del riesgo de la 1ª Línea de Defensa sean apropiados y funcionen correctamente" 3. Ley 1952 de 2019 código general disciplinario, capítulo II – Deberes, artículo 38. Deberes. Son deberes de todo servidor público, numeral 32. Adoptar el Sistema de Control Interno y la función independiente de Auditoría Interna de que trata la Ley 87 de 1993 y demás normas que la modifiquen o complementen.	1. Falta de socialización de los documentos con todas las partes interesadas antes de su publicación. 2.Falta de seguimiento a la aplicación de los procedimientos.	ROPESI-5 Falta de articulación y seguimiento en el mantenimiento y mejora de los sistemas de gestión de la Entidad CTROPESI-9	7,6% (1 actividad no aplicable de las 13 del procedimiento)	Actividades sin responsable de su ejecución en primera y segunda línea de defensa	1 Evaluar las políticas y componentes de seguridad de la información y riesgos de ciberseguridad	1. Desempeño y gestión Institucional	Gestión de Riesgos - Oficial de seguridad de la Información	31/10/2023	1. Catalogo documental : *P-RI-23 monitoreo a la gestión y al gobierno de la seguridad de la información institucional v.03 2023-09-22* 2.Hoja obs 6 3. Memorando radicado nro. 20181200088413 - Solicitud de revisión y modificación de documentos del SGC		

Elaboró:

Auditores - Asesoría de Control Interno: Adriana María Ocampo- contrato 2023561
Celeny González Parra- contrato 2023563
Diego Alexis Ossa- contrato 2023562

Aprobó:

Asesor de Control Interno: Mireya López Ch