

	INSTITUTO NACIONAL DE MEDICINA LEGAL Y CIENCIAS FORENSES	
	INFORME RESUMEN DE AUDITORÍA INTERNA	Página 1 de 5

ID DE LA AUDITORIA:	PROCESO A AUDITAR:	UNIDAD ORGANIZACIONAL:	FECHA DE AUDITORIA:
AI-20-2022	Gestión de la Infraestructura Tecnológica y Servicios informáticos (SUBSISTEMA DE LA SEGURIDAD DE LA INFORMACIÓN)	Grupo Nacional de Tecnologías de Información y Desarrollo (Sede Central) Dirección Regional Norte	Planeación: 2022-11-01 al 2022-11-11 Ejecución: 2022-11-15 al 2022-11-28(1) Elaboración Informe: 2022-11-29 al 2022-12-13(2) Fecha de ajuste informe: 2023-06-16

OBJETIVOS DE LA AUDITORÍA:

1. Evaluar la Oportunidad, el Cumplimiento y la Eficacia de las soluciones de Tecnologías de la Información y Comunicaciones (TIC) que permitan mediante estándares de calidad, seguridad y buenas prácticas, apoyar el cumplimiento de los objetivos institucionales
2. Evaluar el nivel de adopción de la Política de la Seguridad de la Información y el nivel de cumplimiento del Plan Estratégico de Tecnologías de la información y Comunicaciones (PETIC)
3. Evaluar la oportunidad y eficiencia del tratamiento de los riesgos, controles existentes, indicadores y acciones correctivas, preventivas y de mejora, para el fortalecimiento de la gestión institucional.
4. Verificar cumplimiento de los objetivos estratégicos relacionados con el proceso de Gestión de la Infraestructura Tecnológica y Servicios Informáticos.

ALCANCE DE LA AUDITORIA:

En el periodo comprendido entre la última auditorias hasta la fecha de la auditoría.
Para los documentos definidos en la columna denominada "CRITERIOS DE AUDITORIA".
Para las ubicaciones definidas en la columna denominada "UNIDAD(ES) ORGANIZACIONAL".

CRITERIOS DE AUDITORIA:

NTC-ISO 27001:2013

- Numeral 4 Contexto de la Organización
- Numeral 5 Liderazgo
- Numeral 6 Planificación
- Numeral 7 Soporte
- Numeral 8 Operación
- Numeral 9 Evaluación del desempeño
- Numeral 10 Mejora

MIPG- 7A DIMENSIÓN

DOCUMENTOS DEL SIG RELACIONADOS

- DG-A-CARACT-022-V4 - (30-dic-16) - Caracterización del Proceso de Gestión de la Infraestructura Tecnológica y Servicios Informáticos
- DG-A-P-038-V3 - (12-nov-19) - Gestión de incidentes de la Seguridad de la Información,
- DG-A-P-083-V2 - (18-ago-17) - Gestión de incidentes de Tecnologías de la Información
- DG-A-P-111-V1 - (29-nov-19) - Gestión de la Capacidad de las Tecnologías de la Información,
- DG-A-P-109-V1 - (29-nov-19) - Gestión Del Cambio En La Infraestructura De Tecnologías De La Información.

NORMATIVIDAD EXTERNA RELACIONADA

- Decreto No. 1008 de 2018 (junio 14) – Política de Gobierno Digital - Por el cual se establecen los lineamientos generales de la política de Gobierno Digital.
- Decreto No. 1078 de 2015 (26 de mayo) – Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones. Libro 2, parte 2, título 9. Cap. 1.
- RESOLUCION 1519 2020 "Por la cual se definen los estándares y directrices para publicar la información señalada en la Ley 1712 del 2014 y se definen los requisitos materia de acceso a la información pública, accesibilidad web, seguridad digital, y datos abiertos"

NORMATIVIDAD INTERNA RELACIONADA

- Resolución No. 001123 de 2018 – Creación del Comité de Gobierno Digital del INMLCF.
- Resolución No. 000830 de 2019 - (18 de noviembre)– Renovación de los Grupos Internos de trabajo, establecen sus funciones y dictan otras disposiciones -Numeral 1.1
- Resolución No. 000837 de 2019 – Adopción del SGSI INMLCF y la Política de la Seguridad de la Información.
- Resolución No. 000858 de 2019 – Actualización de la Política de Gestión del Riesgo en el INMLCF
- Resolución No. 000017 de 2020 - Política de Privacidad y Protección de Datos Personales en el INMLCF

Y demás normatividad vigente aplicada al proceso a auditar.

AUDITOR LÍDER:	AUDITOR(ES) ACOMPAÑANTE(S)	EXPERTO (S) TÉCNICO(S)	AUDITOR (ES) EN FORMACIÓN
Henry Cortés Contreras	No aplica	Agustín Alberto Torres Agudelo	No aplica

	INSTITUTO NACIONAL DE MEDICINA LEGAL Y CIENCIAS FORENSES	
INFORME RESUMEN DE AUDITORÍA INTERNA		Página 2 de 5

ASPECTOS FAVORABLES	
Durante la evaluación al Proceso de Gestión de la Infraestructura Tecnológica y Servicios Informáticos y el Sistema de Gestión de la Seguridad de la Información se resalta: 1. Proactividad del equipo auditado en suministrar la información necesaria para realizar la fase de Ejecución de la Auditoría. 2. Aplicación del “Procedimiento de Gestión de la Información Digital de la Regional Norte”, Código DRNR-A-I-001- V4 – 2022-04-26 -Anexo V1: 23 marzo de 2022 y del instructivo “Instrucciones para gestión de imágenes NAS del servicio pericial en la Regional Norte - DRNR-A-I-001-AX-001 – cuyo objetivo: Gestionar el manejo de la información para el aseguramiento físico y digital de las actividades que soportan los procesos institucionales. Esta actividad se realiza a través de una herramienta para almacenamiento de información – NAS que permite guardar información misional (imágenes fotográficas) y de apoyo (información almacenada del área administrativa); lo anterior ha permitido un control efectivo de almacenamiento y acceso a dicha información de acuerdo a perfiles definidos. 3. La Gestión realizada desde el Grupo Nacional de Tecnologías de la Información y Desarrollo en el cumplimiento a la “Política de Seguridad Digital” (Resolución 1519 de 2020) establecida por el Gobierno Nacional en los temas como: IPV6, PETIC, aplicación del SGSI.	

NO CONFORMIDAD No. 1	
Descripción:	No se asegura que los bienes entregados a los funcionarios se registren a su nombre, se realicen los traslados correspondientes y se haga seguimiento a los faltantes.
Requisito aplicable:	1. Procedimiento Gestión y Control de los elementos devolutivos en servicio DG-A-P-009 V6 2. DGDG-A-P-019-F-003 - Procedimiento de Solicitud Baja de Elementos Devolutivos Inservibles u Obsoleto. 3. Resolución No.000009 de 2001 Por la cual se establece el procedimiento para la administración de bienes muebles del Instituto Nacional de Medicina Legal y Ciencias Forenses 4. MIPG7ª. DIMENSIÓN- Componentes Actividades de Control
Evidencia objetiva:	En el muestro físico realizado se evidenciaron las siguientes inconsistencias en los inventarios de elementos devolutivos a cargo de los servidores públicos: 1. Elementos Devolutivos Faltantes 2. Elementos Devolutivos Pendientes de dar de baja 3. Elementos devolutivos pendientes de ser trasladados del inventario del Servidor Público a las unidades organizaciones descritas a continuación: 4. Existen elementos devolutivos de servidores públicos que fueron trasladados a otras unidades organizacionales, tales como:

	INSTITUTO NACIONAL DE MEDICINA LEGAL Y CIENCIAS FORENSES	
	INFORME RESUMEN DE AUDITORIA INTERNA	Página 3 de 5

NO CONFORMIDAD No. 2	
Descripción:	Para el Proceso de Gestión de la Infraestructura Tecnológica y Servicios Informáticos y el SGSI, falta por implementar el plan de tratamiento y a su vez, la generación de los informes de monitoreo de los riesgos de la seguridad de la información.
Requisito aplicable:	1. NORMA NTC- ISO 27001:2013 - Numeral 6.1.3 - Tratamiento de los Riesgos de La Seguridad de La Información. 2. Procedimiento De Gestión De Riesgos – Código DG-E-P-022-V7- Actividad No 5 – Monitorear los Riesgos 3. MIPG 7ª. DIMENSIÓN- Componente: Valoración de riesgos
Evidencia objetiva:	Evidencia 1: Dentro de la verificación realizada al módulo de riesgos de seguridad digital se evidenció que se encuentra en proceso de parametrización, verificación y ajuste en el ambiente de producción donde se está gestionando un riesgo asociado a la disponibilidad. Evidencia 2: No se evidencia el “informe de monitoreo de riesgos de seguridad de la información” que se encuentra descrito dentro de la tarea 1 – actividad 5 “monitorear riesgos” del procedimiento de gestión de riesgos.

NO CONFORMIDAD No. 3	
Descripción:	Para el proceso de gestión de la Infraestructura Tecnológica y Servicios Informáticos y el SGSI, en lo relacionado las aplicaciones y Sistemas de Información, no se mantiene la información documentada y actualizada para la eficacia del SGS
Requisito aplicable:	1. NORMA NTC- ISO 27001:2013 - Numeral 7.5.3 - Información Documentada. 2. NORMA NTC- ISO 27001:2013 - Anexo A.12.1.1 y A.12.1.2 – Seguridad de las Operaciones (Procedimientos y Gestión de Cambios). 3. Procedimiento de Control de Documentos – CODIGO DG-E-P-001-V18 – Generalidades. 4. MIPG 7a. DIMENSIÓN- Componente: Actividades de Control.
Evidencia objetiva:	Evidencia 1. En la revisión de efectuada de los manuales de los sistemas de información y aplicaciones, se evidenció que se encuentran sin indicar la versión y la fecha de actualización del mismo Evidencia 2. En la revisión a la documentación asociada al Procedimiento de Infraestructura Tecnológica y Servicios se evidenció documentos se encuentran en estado de borrador y están pendientes la revisión y aprobación

NO CONFORMIDAD No. 4	
Descripción:	Para la aplicación de la Política de Seguridad de la Información no se garantiza la asignación del Líder de Seguridad de la Información que ejerza las funciones descritas en la Resolución.
Requisito aplicable:	1. NORMA NTC- ISO 27001:2013 - NUMERAL 5.3 - ROLES Y RESPONSABILIDADES EN LA ORGANIZACIÓN 2. Resolución No.000837 DEL 22 nov. — 2019 – Artículo 10. Designación del líder de la seguridad de la información. 3. MIPG 7a. DIMENSIÓN- Componente: Ambiente de Control
Evidencia objetiva:	No se evidencia la designación del Líder de Seguridad de la Información por la Alta dirección. Tal como lo establece la Resolución No.000837 de 2019 en su artículo 10, así: “Artículo 10: Designación del Líder de seguridad de la información • La Dirección General asignará la función de Líder de la Seguridad de la información para el ejercicio de las funciones descritas en esta resolución”.

**OPORTUNIDADES DE MEJORA**

Evaluar la posibilidad de considerar los siguientes aspectos que contribuyan al desarrollo del Proceso de Gestión de Infraestructura Tecnológica y Servicios Informáticos y el Sistema de Gestión de la Seguridad de la Información:

1. Verificación de los anexos que son adjuntados a los indicadores asociados al Proceso de Gestión de Infraestructura Tecnológica y Servicios Informáticos.
2. Implementación del uso de la herramienta para almacenamiento de información – NAS para guardar la información misional y de nivel nacional en las direcciones regionales donde aún no se ha aplicado.
3. Que la coordinación del GNTID desagregue actividades en los profesionales con funciones para desarrollo y mejora de aplicaciones institucionales, debido a que se evidenció que dichos servidores públicos tienen a su cargo el desarrollo o mejora de los aplicativos, realización de las pruebas técnicas, cargue a producción las mejoras a los aplicativos, administración la base de datos, activación y desactivación de las aplicaciones, lo que conllevaría a que una sola persona tenga el control total del aplicativo generando un posible riesgo relacionado con la posibilidad alteración o modificación de datos sensibles por excesiva autoridad y control sobre un recurso informático.
4. Incorporación de las mejoras al reporte de ORION relacionado con el informe de disponibilidad, en cuanto a incluirle la simbología del semáforo para los casos que superen la indisponibilidad en un 40%
5. Solicitar a la Oficina de Personal el envío periódico y oportuno de las situaciones administrativas relacionadas con licencias, incapacidades, comisiones, retiros, ingresos y vacaciones las cuales afectan la activación desactivación oportuna de los servidores públicos de los sistemas y aplicaciones institucionales.
6. Que la activación y desactivación de usuarios en las aplicaciones institucionales las realice un servidor público con funciones de administrador de usuarios; para el caso de las aplicaciones misionales, se asigne esta función a los directores regionales a fin de mantener una trazabilidad de autorización de estos eventos. Para cualquiera de las dos opciones, debe realizarse la solicitud de la novedad (activación o desactivación) en forma escrita y registrase en el aplicativo OTRS.
7. Que el GNTID dispongan de participación en la construcción del Plan Estratégico Institucional a fin de articular el Plan Estratégico de Tecnologías de Información (PETIC) acorde a la Política de Gobierno Digital.

CONCLUSIONES DE LA AUDITORÍA

Realizada la auditoría se puede concluir que:

1. Que el Grupo Nacional de Tecnologías de la Información y Desarrollo ha dado cumplimiento oportuno y con eficacia a las soluciones de Tecnologías de la Información y Comunicaciones, siguiendo los estándares de calidad, seguridad y buenas prácticas, apoyando el cumplimiento de los objetivos institucionales.
2. Se dispone de un nivel de adopción de la Política de la Seguridad de la Información, sustentado en los indicadores diseñados para la medición de la política y se viene dando cumplimiento al Plan Estratégico de Tecnologías de la Información y Comunicaciones (PETIC) acorde al presupuesto asignado para esta labor.
3. Se ha realizado un tratamiento adecuado de los riesgos asociados al Proceso de Gestión de la Infraestructura Tecnológica y servicios Informáticos, sin embargo, aún el módulo de Riesgos de Seguridad Digital tiene pendiente la incorporación de los riesgos de confidencialidad e integridad.
4. Se viene dando cumplimiento a los objetivos estratégicos relacionados con el Proceso de Gestión de la Infraestructura Tecnológica y Servicios Informáticos.

	INSTITUTO NACIONAL DE MEDICINA LEGAL Y CIENCIAS FORENSES	
	INFORME RESUMEN DE AUDITORIA INTERNA	Página 5 de 5

5. En la reunión de cierre de la auditoría realizada el día 5 de diciembre de 2022, se concertó con el equipo auditado los hallazgos y oportunidades de mejora del presente informe.

Se realizó parte de la etapa de ejecución en forma remota y presencial utilizando las herramientas autorizadas por el GNTID para efectuar las entrevistas y grabaciones y mediante revisión documental aplicando el protocolo de roles para la realización de Auditorías Remotas en el INMLCF, se enviaron las invitaciones a todos los participantes de la auditoría de acuerdo a las direcciones de correo institucional (dichos invitados fueron previamente concertados con el líder del proceso), se definió claramente el tiempo de inicio y finalización de la cada actividad de conexión remota, aplicando 100% la herramienta de Google Meet, autorizada por Instituto; la comunicación fue óptima y los dispositivos utilizados no tuvieron ningún contratiempo.

ANEXOS DE LA AUDITORÍA
Las evidencias descritas en el informe y demás papeles de trabajo se encuentran en el archivo digital de la Auditoria AI-20-2022.

REGISTRO DE HORAS					FECHA
NOMBRE(S) DEL EQUIPO AUDITOR		NORMA NTC/ISO/IEC 27001:2013	MIPG 7 ^a DIMENSION	OTRAS	2023-07-04 ACCIONES CORRECTIVAS Y PREVENTIVAS
AL:	HENRY CORTES CONTRERAS	80	80	N/A	
AA1:	N/A	N/A	N/A	N/A	
AA2:	N/A	N/A	N/A	N/A	
AA3:	N/A	N/A	N/A	N/A	
ET1:	AGUSTIN ALBERTO TORES	80	80	N/A	
ET:	N/A	N/A	N/A	N/A	
 FIRMA DE AUDITORES					INFORME DE AUDITORÍA 2023-06-16