



INSTITUTO NACIONAL DE MEDICINA LEGAL Y CIENCIAS FORENSES

INFORME RESUMEN DE AUDITORÍA

Página 1 de 38

ID DE LA AUDITORIA:	PROCESO A AUDITAR:	UNIDAD ORGANIZACIONAL:	FECHA DE AUDITORIA:
AI-08-2023	Gestión de la Infraestructura Tecnológica y Servicios Informáticos – Sistema de la Seguridad de la Información)	Subdirección Administrativa y Financiera Grupo Nacional de Tecnologías de Información y Desarrollo (Sede Central) Oficina de Personal – Grupo Nacional de Registro y Control Demás roles involucrados en el proceso auditado	Planeación: 2023-07-31 al 2023-08-04 Ejecución: 2023-08-08 al 2023-08-18 Informe: 2023-08-22 al 2023-09-05

OBJETIVOS DE LA AUDITORIA:

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 asociados a la disponibilidad, confidencialidad e integridad de la información del aplicativo SIAF módulo nómina.
4. Evaluar la efectividad de las acciones incluidas en los planes de mejoramiento (acciones preventivas y acciones correctivas) producto de las auditorías internas.
5. Evaluar la efectividad de los controles de los riesgos asociados al proceso auditado.
6. Verificar cumplimiento de los objetivos estratégicos relacionados con el proceso auditado.

ALCANCE DE LA AUDITORIA:

En el periodo comprendido entre la última auditoria hasta la fecha de la presente auditoria, para los documentos definidos en la columna denominada "CRITERIOS DE AUDITORIA" y las definidas en la columna denominada "UNIDAD(ES) ORGANIZACIONAL".

Se evaluarán las operaciones realizadas en el aplicativo SIAF - Módulo de nómina desde el 01 de enero de 2023 hasta la fecha de la presente auditoria.

CRITERIOS DE AUDITORIA:

NTC-ISO 27001:2013 Numerales: 4, 5, 6, 7, 8, 9 y 10, MIPG – 7ª Dimensión

DOCUMENTOS DEL SIG RELACIONADOS

DG-A-CARACT-022 Caracterización del Proceso de Gestión de la Infraestructura Tecnológica y Servicios Informáticos

DG-A-P-038 Gestión de incidentes de la Seguridad de la Información

DG-A-P-083 Gestión de incidentes de Tecnologías de la Información

DG-A-P-111 Gestión de la Capacidad de las Tecnologías de la Información

DG-A-P-110 Gestión de la disponibilidad de las tecnologías de la información

DG-A-P-109 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) – Por la cual se actualizan los grupos internos de trabajo y se establecen sus funciones y dictan otras disposiciones.

Resolución No. 000607 de 2022 - (6 de julio) – Eliminación y creación de grupos internos de trabajo del INMLCF – Numeral 4.8. Resolución No. 001142 de 2022 – (29 de diciembre) – Actualización de la política de gestión del Riesgo

Resolución No. 000017 de 2020 - Política de Privacidad y Protección de Datos Personales en el INMLCF
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

Acuerdo 08 de 2012 “Por la cual se desarrolla la estructura interna del Instituto Nacional de Medicina Legal y Ciencias Forenses y se establecen funciones”.

Resolución No. 000172 de 2023 – Por la cual se actualizan los grupos internos de trabajo, establecen sus funciones y dictan otras disposiciones.

Y demás normatividad vigente aplicada al proceso a auditar.

CAMBIOS (SI APLICA)

Se incluyó el Objetivo No. 3 “Evaluar la oportunidad y eficiencia del tratamiento de los riesgos asociados a la disponibilidad, confidencialidad e integridad de la información del aplicativo SIAF módulo nómina”.

Se modifican fechas de ejecución programadas en el PUNAS inicial.

En la reunión de apertura y plan de auditoría se informa que “Adicional al módulo de nómina del SIAF, se seleccionarán sistemas de información misionales para verificar controles de seguridad de la información”.

**INSTITUTO NACIONAL DE MEDICINA LEGAL Y CIENCIAS FORENSES****INFORME RESUMEN DE AUDITORÍA**

Página 3 de 38

AUDITOR LÍDER:	AUDITOR(ES) ACOMPAÑANTE(S)	EXPERTO (S) TÉCNICO (S)	AUDITOR (ES) EN FORMACIÓN
NESTOR JAVIER CARDENAS VARGAS	DIANA MARIA FLOREZ VALENCIA HUGO ALONSO PEREZ CARVAJAL JAIRO ALEXANDER ESTUPIÑAN ALVARADO WILMER ALEXANDER BARACALDO CIFUENTES	NO APLICA	NO APLICA

A continuación se presentan las no conformidades y un resumen de los aspectos favorables y evidencias de la Auditoría al Proceso AI-08-2023, así como la conclusión registrada en el informe original.

ASPECTOS FAVORABLES

1. Se resalta la disponibilidad de todos los funcionarios auditados durante el desarrollo de la Auditoría.
2. Se destaca que la Dirección del Instituto Nacional de Medicina Legal y Ciencias Forenses, le da importancia al sistema de gestión en seguridad de la información, al autorizar una auditoría interna con una entidad externa, con el fin de verificar controles y posibles vulneraciones que puedan tener los diferentes sistemas de información de la entidad.
3. Es de relevancia señalar las competencias y conocimientos del personal del Grupo Nacional de Tecnologías de Información y Desarrollo del INMLCF y de cada uno de los auditados.

DESCRIPCIÓN DE HALLAZGOS**NO CONFORMIDAD No. 1**

Descripción:	El Instituto Nacional de Medicina Legal y Ciencias Forenses, no asegura que las políticas de seguridad de la información específicas sean adecuadas para el propósito de la organización.
Requisito aplicable:	1. NTC-ISO/IEC 27001:2013. Tecnología de la información. Técnicas de seguridad. Sistemas de Gestión de la Seguridad de la Información. Requisitos. Numeral 5.2. Política; anexo A "Objetivos de control y controles de referencia", A.5.1.1 "Políticas para la Seguridad de la información"; "control", A.6.2.1, A.9.1.1, A.10.1.1, A.11.2.9, A.13.2.1, A.14.2.1, A.15.1.1. 2. Resolución No. 000837 del 22/11/2019, por la cual se adopta el Sistema de Gestión de la Seguridad de la Información- SGSI, la política de seguridad de la información y se establecen lineamientos para su uso y manejo, artículo 3. 3. Anexo manual de políticas de la seguridad de la información versión 3 de 28/01/2020.



INSTITUTO NACIONAL DE MEDICINA LEGAL Y CIENCIAS FORENSES

INFORME RESUMEN DE AUDITORÍA

Página 4 de 38

	4. Manual del Sistema Integrado de Gestión (DG-MANUAL-001) versión 15, numeral 7 “Política del Sistema Integrado de Gestión (SIG)”. 5. Matriz declaración de Aplicabilidad Sistema de Gestión de Seguridad de la Información de fecha 12/12/2018, A.6.2.1, A.9.1.1, A.10.1.1, A.11.2.9, A.13.2.1, A.14.2.1, A.15.1.1. 6. MIPG 7ª. DIMENSIÓN- Componentes Actividades de Control.
Evidencia objetiva:	Teniendo en cuenta que el Instituto Nacional de Medicina Legal y Ciencias Forenses (INMLCF) estableció en su declaración de aplicabilidad el cumplimiento de los 114 controles de la norma, se verificó la Política de Seguridad de la Información General y Específicas del INMLCF; sin embargo, la entidad no tiene definidas las políticas específicas, tales como; Dispositivos Móviles, Política Control de Acceso, Política sobre el uso de Controles Criptográficos, Política de Escritorio Limpio y Pantalla Limpia, Políticas y Procedimientos de Transferencia de la información, Política de Desarrollo Seguro y Política de Seguridad de la Información para la Relación con Proveedores que Brinden Orientación y Soporte, por parte de la dirección, para la seguridad de la información de acuerdo con los requisitos del negocio y con las leyes y reglamentos pertinentes. Se confirmó que en el documento “Anexo Manual de Políticas para la Gestión de Seguridad de la Información del Instituto Nacional de Medicina Legal y Ciencias Forenses” que se encuentra en el sistema de información ISOLUCION, el INMLCF registró como políticas, todos los controles relacionados desde el numeral A5 hasta el A18 sin estar definidas, por ende, no están documentados los objetivos que permitan ejecutar el desarrollo y cumplimiento de las mismas. Lo anterior, según lo relacionado en la Resolución No. 000837 del 22/11/2019, del INMLCF “por la cual se adopta el Sistema de Gestión de la Seguridad de la Información-SGSI, la Política de Seguridad de la Información y se establecen lineamientos para su uso y manejo”, en su artículo 3 “Políticas y Lineamientos de la Seguridad de la Información” donde se establece que en un documento anexo se encuentra el detalle de las demás políticas, así: “...se adopta como parte integral de este acto administrativo el documento anexo denominado “Anexo Manual de Políticas para la Gestión de Seguridad de la Información del Instituto Nacional de Medicina Legal y Ciencias Forenses”, como instrumento principal donde se encuentra el detalle de las políticas y lineamientos de la seguridad de la información...”

NO CONFORMIDAD No. 2

Descripción:	El Comité de Gobierno Digital establecido por el Instituto Nacional de Medicina Legal y Ciencias Forenses, no cumple con la revisión del SGSI para asegurar que la seguridad de información se implemente y opere de acuerdo con las políticas y procedimientos organizacionales, asegurando su conveniencia, adecuación y eficacia continua
Requisito aplicable:	1. NTC-ISO/IEC 27001:2013. Tecnología de la información. Técnicas de seguridad. Sistemas de Gestión de la Seguridad de la Información. Requisitos. anexo A “Objetivos de control y controles de referencia”, A.5.1.2. “revisión de

**INSTITUTO NACIONAL DE MEDICINA LEGAL Y CIENCIAS FORENSES****INFORME RESUMEN DE AUDITORÍA**

Página 5 de 38

	las Políticas para la seguridad de la información”, A.18.2. “revisiones de seguridad de la información”. 2. Resolución No. 000837 del 22/11/2019, por la cual se adopta el Sistema de Gestión de la Seguridad de la Información-SGSI, la política de seguridad de la información y se establecen lineamientos para su uso y manejo, artículo 7 “revisión de la política de la seguridad de la información”; artículo 8 “roles y responsabilidades de los intervinientes en la organización de la seguridad de la información”, literal 3 “Comité de gobierno digital”. 3. Resolución 001123 del 12/12/2018, por la cual se crea el Comité de Gobierno Digital del Instituto Nacional de Medicina Legal y Ciencias Forenses y se dictan otras disposiciones. 4. MIPG7^a. DIMENSIÓN- Componentes: Ambiente de Control y Actividades de Control.
Evidencia objetiva:	Mediante correo electrónico, el día 09/08/2023, se solicita a la secretaria técnica del Comité de Gobierno Digital, precedido por el Grupo Nacional de Atención y Servicio al Ciudadano del INMLCF, el soporte (acta de reunión) de las dos (2) últimas sesiones o reuniones llevadas a cabo por el Comité de Gobierno Digital vigencia 2022 y 2023, con el fin de verificar las revisiones o actualizaciones de las políticas de seguridad de la información; así como también, los temas estratégicos tratados en relación con la seguridad de la información y sus recomendaciones, de lo anterior se evidenció que las dos (2) últimas sesiones realizadas por este comité fueron el 2020/07/24 y 2020/08/14, en las cuales no se trató la revisión anual de políticas de la seguridad de información establecida en el artículo 7 de la Resolución No. 000837 del 22/11/2019, así como tampoco, temas estratégicos en relación con la seguridad de la información, incumpliendo las directrices institucionales y el control A.5.1.2, que dice: “...las políticas para la seguridad de la información se deben revisar a intervalos planificados, o si ocurren cambios significativos,”

NO CONFORMIDAD No. 3

Descripción:	El Grupo Nacional de Tecnologías de la Información y Desarrollo del Instituto Nacional de Medicina Legal y Ciencias Forenses, no aplica adecuadamente el análisis de causas para las no conformidades reales evidenciadas en la vigencia 2022, conforme a las metodologías definidas por la entidad.
Requisito aplicable:	1. NTC-ISO/IEC 27001:2013. Tecnología de la información. Técnicas de seguridad. Sistemas de Gestión de la Seguridad de la Información. Requisitos. Numeral 10 “mejora”. 2. Documento anexo “metodología para abordar la no conformidad, su análisis de causas, implementación y evaluación de eficacia (DG-C-P-014-AX-004)”, versión 13. 3. MIPG7^a. DIMENSIÓN- Componentes Actividades de Control
Evidencia objetiva:	Tomando como muestra el análisis de causa realizado por el Grupo Nacional de Tecnologías de la Información y Desarrollo a las no conformidades No.2977 y

No.2980 del informe de auditoría interna AI-20-2022, encontrando que no se lleva a cabo la metodología establecida de los “POR QUÉ” por la entidad en su documento DG-C-P-014-AX-004 versión 13, donde, la técnica consiste en realizar cuantas veces sea necesario ¿Por qué? hasta agotar las preguntas posibles e identificar la causa raíz del problema.

Asimismo, la entidad determinó la forma de utilizar la metodología de la siguiente manera:

- Identificar el problema a solucionar.
- Establecer el equipo de trabajo acorde con lo mencionado en el paso 2. Esta técnica se utiliza mejor en equipos pequeños (5 a 10 personas)
- Definir un moderador. Es importante que esta persona sea conocedora de la dinámica del equipo y los miembros del mismo. Teniendo en cuenta que es probable que se puedan presentar diferencias entre los involucrados.
- Se recomienda iniciar con una lluvia de ideas que permita establecer las causas del problema, esta técnica permite obtener un gran número de ideas sobre el problema en estudio. Lo más importante es no desechar en un principio, ninguna de ellas. Luego por votación, se depura la lista inicial hasta que se escogen las más representativas.
- Preguntar al menos 5 veces, ¿Por qué es así...? o ¿Por qué está pasando esto? Cada pregunta logra avanzar sobre un nivel de detalle, hasta que se logre identificar la causa raíz.
- El escalar en los niveles de detalle permita al grupo ahondar sobre las causas del problema, consolidando información precisa sobre el mismo. En cuanto más se trabaje en profundidad sobre cada nivel y se busque consolidar uno nuevo, se asegurará la identificación de la causa raíz del problema.” (Tomado de: DG-C-P-014- AX-004 “METODOLOGÍA PARA ABORDAR LA NO CONFORMIDAD, SU ANÁLISIS DE CAUSAS, IMPLEMENTACIÓN Y EVALUACIÓN DE EFICACIA.”, versión 13)

Sin embargo, no se observó lo siguiente en el acta análisis de causas del 30/06/2023:

- Equipo de trabajo de 5 a 10 personas, donde sólo se evidenciaron tres funcionarios.
- Iniciar con lluvia de ideas que permita establecer las causas del problema, permitiendo obtener un gran número de ideas sobre el problema en estudio, luego por votación, se depura la lista hasta escoger la más representativa.
- Preguntar al menos 5 veces, ¿Por qué es así...? O ¿Por qué está pasando esto?

A continuación, se registra el análisis de causas realizado por la unidad en el acta del 30/06/2023 y lo registrado en el sistema de información ISOLUCION con fecha 12/07/2023, así:

2. Análisis de causas

☐ Espina de Pescado ☒ Porques

Porques

Porqué 1

No se ha realizado la toma física general de inventarios de elementos devolutivos.

Porqué 2

no aplica

Porqué 3

no aplica

Porqué 4

no aplica

Porqué 5

no aplica

No conformidad real	Descripción No conformidad	Causa establecida	Porqués valorados para el análisis
No.2977	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.	No se ha realizado la toma física general de inventarios de elementos devolutivos.	Uno (1)
No.2980	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	No se ha designado por parte de la Alta Dirección el líder de seguridad de la información	Uno (1)

Registro Fotográfico:

Análisis de causa NC No.2977 (ISOLUCION)

2. Análisis de causas

☐ Espina de Pescado ☒ Porques

Porques

Porqué 1

No se ha designado por parte de la Alta Dirección el líder de seguridad de la información

Porqué 2

no aplica

Porqué 3

no aplica

Porqué 4

no aplica

Porqué 5

no aplica

**Análisis de causa NC No.2980 (ISOLUCION)****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.

Causa No se ha realizado la toma física general de inventarios de elementos devolutivos.

Registro análisis de causa NC No.2977 según acta de reunión de fecha 30/06/2023.

NO CONFORMIDAD No. 4**Descripción:**

La Declaración de Aplicabilidad para el SGSI del INMLCF no se encuentra actualizada, aprobada y publicada; asimismo, no se establece la implementación y la gestión de controles necesarios para mitigar el riesgo en cada uno de los 114 controles adoptados por la entidad.

Requisito aplicable:

1. NTC-ISO/IEC 27001:2013. Tecnología de la información. Técnicas de seguridad. Sistemas de Gestión de la Seguridad de la Información. Requisitos. Numeral 4.3. "Determinar del alcance del sistema de gestión de la seguridad de la información" y anexo A "objetivos de control y controles de referencia".
2. Anexo manual de políticas de seguridad de la información, numeral 5 al 18.
3. Declaración de Aplicabilidad Sistema de Gestión de Seguridad de la Información de fecha 12/12/2018, numeral 5 al 18.
4. MIPG7^a. DIMENSIÓN- Componentes: Ambiente de Control, Evaluación del riesgo y Actividades de Control.

Evidencia objetiva:

Una vez revisada la declaración de aplicabilidad del sistema de seguridad de la información del Instituto Nacional de Medicina Legal y Ciencias Forenses, ubicada en la carpeta compartida "PLAN AUDITORIA INTERNA AI-08-2023" asignada por el instituto para el cargue de los soportes de auditoria mediante archivo en formato Excel denominado "Declaracion_Aplicabilidad-v1-2019_01-28 (2)", se observó que el documento en mención no se encuentra actualizado desde el 12/12/2018, no ha sido aprobado por la Dirección de la entidad y no está publicado, ni comunicado a sus empleados, ni partes externas pertinentes; de igual forma, no establece para cada control la aplicabilidad en el INMLCF, ni el criterio, formato, procedimiento, guía, etc., mediante el cual la entidad demuestra el cumplimiento de cada control, tal como se ejemplifica en la siguiente tabla:

No. Del Control	Control	Descripción del Control	Aplica: SI/NO	DECLARACIÓN DE APLICABILIDAD-INSTITUTO NACIONAL DE MEDICINA LEGAL Y CIENCIAS FORENSES	Evidencia
A.6.2	Dispositivos móviles y teletrabajo				
A.6.2.1	Política para dispositivos móviles*	Control: Se deben adoptar una política y unas medidas de seguridad de soporte, para gestionar los riesgos introducidos por el uso de dispositivos móviles.	SI	Se cuenta con el Manual de Políticas de la Información. Está considerado en la Política SGSI-.6.2.1	Anexo Manual de Políticas de Seguridad de la Información
A-6.2.2	Teletrabajo**	Control: Se deben implementar una política y unas medidas de seguridad de soporte, para proteger la información a la que se tiene acceso, que es procesada o almacenada en los lugares en los que se realiza teletrabajo.	SI	Se cuenta con el Manual de Políticas de Seguridad de la Información. Está considerado en la Política SGSI-A.6.2.2	Anexo Manual de Políticas de Seguridad de la Información.
				La Oficina de Personal cuenta con el documento de Teletrabajo en el Instituto.	Documento de Teletrabajo
				La Oficina de Personal cuenta con Resolución mediante el cual adopta el teletrabajo en el Instituto.	Resolución mediante la cual adopta el teletrabajo en el Instituto.

- No tiene adoptada la política para dispositivos móviles.
- No existe política de teletrabajo, la Oficina de Personal no cuenta con un documento que establezca las condiciones de Teletrabajo en el Instituto; asimismo, el 05/07/2023 la Dirección de la entidad, expide un Memorando donde se finaliza con la emergencia sanitaria y se indica el cumplimiento a la Resolución No. 000488 del 30/06/2019, por la cual se reglamenta la jornada laboral al interior de la entidad.

NO CONFORMIDAD No. 5

Descripción:

El INMLCF no garantiza la implementación y la operacionalización de la seguridad de la información dentro de la entidad con los contratistas, al no asegurar que los riesgos se identifiquen y traten en los diferentes contratos celebrados entre la institución y las empresas.

Requisito aplicable:

1. NTC-ISO/IEC 27001:2013. Tecnología de la información. Técnicas de seguridad. Sistemas de Gestión de la Seguridad de la Información. Requisitos. Anexo A “objetivos de control y controles de referencia” A.6.1.5. “Seguridad de la información en la gestión de proyectos”.
2. Instructivo Gestión de acceso (DG-A-I-057), versión 2.
3. Instructivo control de acceso a las áreas restringidas del Instituto Nacional de Medicina Legal y Ciencias forenses (DG- M-I-115) versión 3.
4. Matriz declaración de Aplicabilidad Sistema de Gestión de Seguridad de la Información de fecha 12/12/2018, A.6.1.5. “Seguridad de la información en la gestión de proyectos”.
5. Anexo manual de políticas de seguridad de la información, Política SGSI-A.6.1.5.

6. MIPG7^a. DIMENSIÓN- Componentes: Evaluación del Riesgo y Actividades de Control

Verificado el Contrato 232-SG-2022 celebrado entre el Instituto Nacional de Medicina Legal y Ciencias Forenses y la firma comisionista COMIAGRO S.A con NIT: 800206442-1, cuyo objeto es “CONTRATAR UNA SOCIEDAD COMISIONISTA MIEMBRO DE LA BOLSA MERCANTIL PARA LA CELEBRACIÓN DE OPERACIONES A TRAVÉS DEL MERCADO DE COMPRAS PÚBLICAS ASÍ: CAPITULO I. PRESTAR EL SERVICIO DE VIGILANCIA Y SEGURIDAD PRIVADA INCLUYENDO ARMAMENTO, ELEMENTOS Y EQUIPOS NECESARIOS PARA LA CUSTODIA DE LOS BIENES MUEBLES E INMUEBLES, ASÍ COMO PARA LA SEGURIDAD DE LOS FUNCIONARIOS Y USUARIOS EN LAS SEDES DEL INSTITUTO NACIONAL DE MEDICINA LEGAL Y CIENCIAS FORENSES A NIVEL NACIONAL, Y CAPITULO II PRESTACION DEL SERVICIO DE ASEO Y CAFETERIA EN LAS INSTALACIONES DEL INSTITUTO NACIONAL DE MEDICINA LEGAL Y CIENCIAS FORENSES A NIVEL NACIONAL” y plazo de ejecución, que será hasta el 31 de agosto de 2026, donde no se evidenció lo siguiente:

- La inclusión de los objetivos de la seguridad de la información en el contrato en mención, estudio previo del proceso y ficha técnica de negociación de la operación del servicio de vigilancia privada y del servicio de Aseo y Cafetería.
- No se establece la valoración de los riesgos de seguridad de la información, para identificar los controles necesarios.
- No se definen las responsabilidades y roles en seguridad de la información

Adicionalmente, se observó en el numeral 9. obligaciones de la sociedad comisionista vendedora y comitente vendedor de la ficha técnica de negociación en la prestación del servicio de aseo y cafetería, los dos siguientes literales:

“j) Ejecutar su actividad con ajuste a los principios de (i) integridad y confianza; (ii) cumplimiento de lo acordado; (iii) lealtad; (iv) trato justo con los clientes; (v) confidencialidad; y, (vi) profesionalismo, según se encuentran previstos en el Capítulo Tercero del Título Primero del Libro Quinto del Reglamento de Funcionamiento y Operación de la BMC.

r) El Comisionista se compromete a guardar la confidencialidad y reserva debida sobre la información que conozca o que le sea suministrada o que resulte del desarrollo del servicio contratado, en consecuencia, cualquier información que el Comisionista conozca de la ENTIDAD debe ser aplicada y utilizada en las condiciones que éste último le haya impartido para su correcto uso. Por tanto, toda información confidencial, secreta o privilegiada que el Comisionista obtenga o conozca de la ENTIDAD debe permanecer con la misma calidad y ser guardada en condiciones tales de reserva y privilegio durante la ejecución y después de liquidado el contrato Guardar reserva de las operaciones ejecutadas en desarrollo del Contrato de Comisión y de sus resultados.”

Evidencia
objetiva:



Igualmente, en el numeral 75 de las obligaciones especiales del comitente vendedor, se establece lo siguiente:

“75) Incluir dentro de los contratos laborales con cada uno de los vigilantes una cláusula de confidencialidad en el manejo de la información de aquellos eventos que llegare a conocer y manejar en desarrollo del contrato. “

Por otro lado, se solicitó mediante correo electrónico de fecha 14/08/2023, los soportes de confidencialidad firmados por cada uno de los empleados de las empresas contratistas, donde el Coordinador del Grupo Nacional de Gestión Administrativa (E) SAF, respondió al requerimiento lo siguiente:

“... Con relación al documento soporte de confidencialidad de cada uno de las personas que prestan el servicio de vigilancia privada y de aseo y cafetería, en las instalaciones del INML y CF, se informa que la documentación, hace parte de los documentos internos de la empresa operadora, a la cual le trasladamos la solicitud, para que en un término no mayor a cinco (5) días, alleguen esa información para compartirla inmediatamente con usted, adicionalmente en los estudios previos y ficha técnica de negociación, se puede verificar, que dentro de las obligaciones del comitente vendedor, debe incluir dentro de los contratos laborales con cada una de las personas operarias de la prestación del SERVICIO DE VIGILANCIA PRIVADA Y ASEO Y CAFETERÍA, una cláusula de confidencialidad en el manejo de la información de aquellos eventos que llegare a conocer y manejar en desarrollo del contrato...”

Por lo tanto, el INMLCF no asegura que el personal de contratistas se integre al SGSI del instituto, no reposa el acuerdo de confidencialidad (DG-A-I-057-F-003) de estos empleados en la entidad, incumpliendo el literal 6 y 11 del numeral 7.5. acuerdos de confidencialidad definidos en el instructivo “gestión de acceso”, que dice:

“6. Para el personal contratistas el acuerdo de confidencialidad deberá reposar en el respectivo contrato celebrado con el instituto Nacional de Medicina Legal y Ciencias Forenses.

11. El Coordinador de la unidad organizacional o quien este delegue, será el responsable de hacer firmar el acuerdo de confidencialidad del personal contratista que tenga a su cargo y de que se encuentre debidamente archivado en el área o en el contrato correspondiente, según sea el caso ”

NO CONFORMIDAD No. 6**Descripción:**

El INMLCF no establece adecuadamente la separación de deberes y responsabilidades entre los grupos y dependencias para evitar y reducir posibles modificaciones no autorizadas, intencionales o uso indebido de los activos de la entidad.

Requisito aplicable:

1. NTC-ISO/IEC 27001:2013. Tecnología de la información. Técnicas de seguridad. Sistemas de Gestión de la Seguridad de la Información. Requisitos. Anexo A “objetivos de control y controles de referencia”, control A.6.1.2 “separación de deberes”.



	2. Anexo manual de políticas de seguridad de la información, Política SGSI-A.6.1.2. 3. Matriz declaración de Aplicabilidad Sistema de Gestión de Seguridad de la Información de fecha 12/12/2018, numeral A.6.1.2. 4. MIPG7^a. DIMENSIÓN- Componentes: Ambiente de Control y Actividades de Control.
Evidencia objetiva:	En visita realizada al Grupo Nacional de Tecnologías de la Información y Desarrollo, y una vez verificado el funcionamiento de algunos de los sistemas de información que maneja el INMLCF, se pudo evidenciar que la administración funcional y técnica de los sistemas de información SICLICO y SIRDEC son funciones y responsabilidades realizadas por el mismo funcionario, por lo cual no se evidencia una adecuada segregación de deberes, teniendo en cuenta que no existe un ambiente de control ni actividades de control de los cambios o desarrollos que se adelanten por parte de este funcionario dentro de los sistemas de información antes mencionados. Por ende, los controles de autorización no se encuentran segregados con el fin de considerar el seguimiento de las actividades realizadas dentro de los mismos como son log's de auditoría y supervisión

NO CONFORMIDAD No. 7

Descripción:	El INMLCF no cuenta con el procedimiento establecido para mantener documentado y/o actualizado los contactos con las autoridades y grupos de interés especial en seguridad de la información.
Requisito aplicable:	1. NTC-ISO/IEC 27001:2013. Tecnología de la información. Técnicas de seguridad. Sistemas de Gestión de la Seguridad de la Información. Requisitos. Anexo A "Objetivos de control y controles de referencia", control A 6.1.3 y A 6.1.4. 2. Anexo manual de políticas de seguridad de la información, Política SGSI - A 6.1.3 y Política SGSI - A 6.1.4. 3. Matriz declaración de Aplicabilidad Sistema de Gestión de Seguridad de la Información de fecha 12/12/2018, A.6.1.3 y A.6.1.4. 4. MIPG7^a. DIMENSIÓN- Componente Actividades de Control
Evidencia objetiva:	Una vez verificado el sistema de información ISOLUCION y página web del INMLCF no se encuentra el procedimiento, ni los directorios en referencia; asimismo, se consultó al Grupo Nacional de Tecnologías de la Información y Desarrollo, sobre la existencia de estos procedimientos y directorios, a lo cual manifestaron, que la entidad no cuenta con estos documentos, como por ejemplo: organismos de supervisión y control, empresas de servicios públicos, servicios de emergencia, proveedores de internet, electricidad, salud, seguridad u otras autoridades pertinentes. Asimismo, grupos de interés especial apropiados como membresías de seguridad, foros de seguridad, asociaciones profesionales especializadas en seguridad o suscripciones con CSIRT, etc.

**NO CONFORMIDAD No. 8****Descripción:**

El INMLCF no cuenta con los controles suficientes para minimizar los riesgos en los que se pueda comprometer la información de la entidad en los dispositivos móviles como son la restricción para la instalación de software, protección contra software malicioso, la deshabilitación de escritorio remoto, entre otros.

Requisito aplicable:

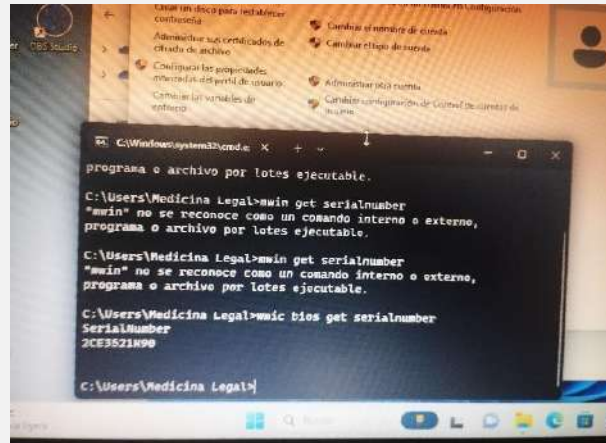
1. NTC-ISO/IEC 27001:2013. Tecnología de la información. Técnicas de seguridad. Sistemas de Gestión de la Seguridad de la Información. Requisitos. Anexo A "Objetivos de control y controles de referencia", control A 6.2.1.
2. Anexo manual de políticas de seguridad de la información, Política SGSI - A 6.2.1.
3. Matriz declaración de Aplicabilidad Sistema de Gestión de Seguridad de la Información de fecha 12/12/2018, A.6.2.1.
4. MIPG7^a. DIMENSIÓN- Componentes: Evaluación del Riesgo y Actividades de Control

Evidencia objetiva:

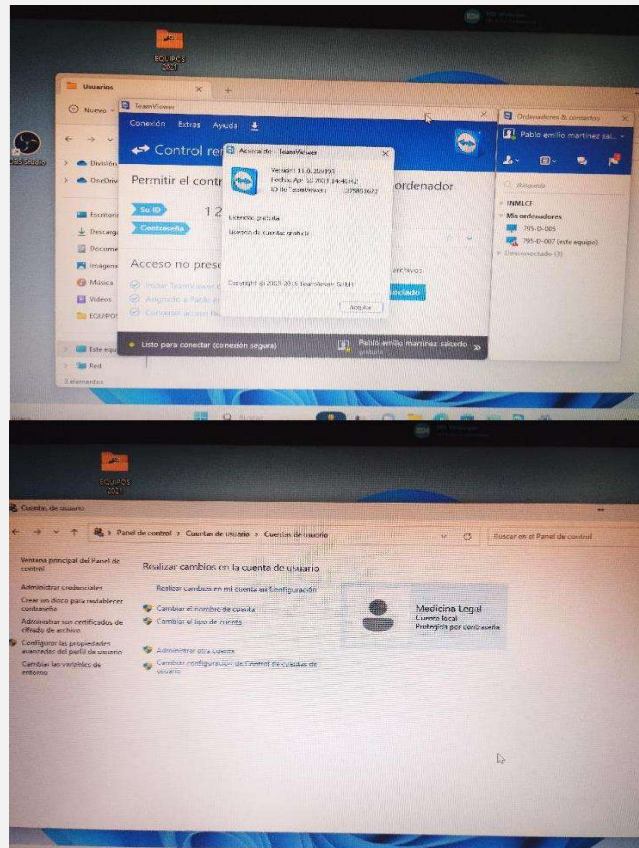
De forma aleatoria, se tomó como muestra el portátil marca HP de serie 2CE3521K90, con el fin de verificar el cumplimiento a la política de dispositivos móviles exigibles por la norma, encontrando que en el INMLCF no se aplican los siguientes controles para proteger la confidencialidad, la autenticidad y/o la integridad de la información:

- Restricciones para instalación de software: el equipo presenta un software instalado no licenciado por la entidad.
- Controles de acceso: el equipo se encuentra con un usuario local-administrador "medicina legal", lo cual no permite controlar los cambios ejecutados dentro del equipo o evitar una afectación a los activos de la entidad.
- Técnicas criptográficas: el equipo no tiene protección criptográfica o cifrado de discos para la protección de la información
- Protección contra software malicioso: el equipo no cuenta con una protección antivirus.
- Deshabilitación remota, borrado o cierre: el equipo no tiene deshabilitada la opción de escritorio remoto.

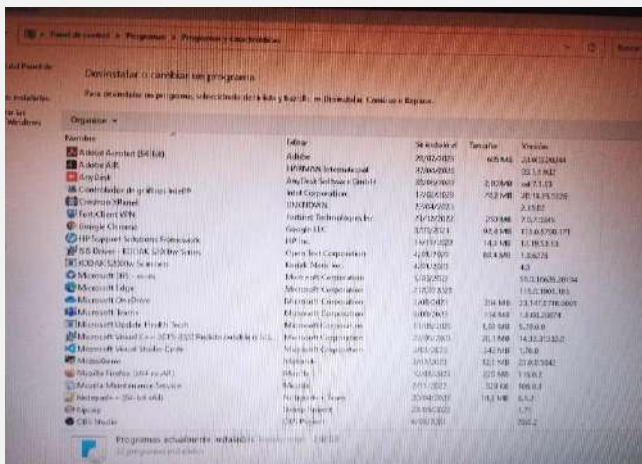
Computador Portátil con serie **2CE3521K90**



No hay restricción para instalación de software



No hay control de acceso, ni protección criptográfica



NO CONFORMIDAD No. 9

Descripción:

El INMLCF no cuenta con una trazabilidad de los eventos (auditorías/logs) realizados dentro de los sistemas de información SICLICO y SIRDEC con el fin de verificar o validar la efectividad del procedimiento de cancelación de usuarios a los funcionarios que han terminado el vínculo laboral con la entidad.

Requisito aplicable:

1. NTC-ISO/IEC 27001:2013. Tecnología de la información. Técnicas de seguridad. Sistemas de Gestión de la Seguridad de la Información. Requisitos. Anexo A "Objetivos de control y controles de referencia", control A 7.3.1.
2. Anexo Manual de políticas de seguridad de la información, Política SGSI - A 7.3.1.
3. Declaración de Aplicabilidad Sistema de Gestión de Seguridad de la Información de fecha 12/12/2018, 7.3.1.
4. MIPG7ª. DIMENSIÓN- Componente Actividades de Control.

Evidencia objetiva:

Se tomó como muestra a los señores OSCAR ARMANDO SANCHEZ CARDOZO, con identificación Nro. 19.442.387, quién terminó su vínculo laboral el 2023/07/13 y RICARDO SANCHEZ SEGURA, con identificación Nro.19.434.015, quién terminó su vínculo laboral el 2023/07/31. Posteriormente, en entrevista con los administradores de los sistemas de información SICLICO y SIRDEC, se revisó el procedimiento de cancelación de usuarios a los funcionarios en mención, sin lograr evidenciar un registro de los eventos o acciones donde fueron deshabilitados o cancelados los usuarios, para determinar el momento exacto o marca temporal (fecha, hora, minuto, segundo) en el que ocurrió.

	INSTITUTO NACIONAL DE MEDICINA LEGAL Y CIENCIAS FORENSES	
	INFORME RESUMEN DE AUDITORÍA	Página 16 de 38

NO CONFORMIDAD No. 10	
Descripción:	El INMLCF no garantiza el etiquetado de la información, de acuerdo al esquema de clasificación de la información adoptado por la entidad, según el índice de información clasificada y reservada que se encuentra publicada en la página web del instituto.
Requisito aplicable:	1. NTC-ISO/IEC 27001:2013. Tecnología de la información. Técnicas de seguridad. Sistemas de Gestión de la Seguridad de la Información. Requisitos. Anexo A “Objetivos de control y controles de referencia”, A.8.2.2. “etiquetado de la información”. 2. Ley 1712 del 06 de marzo de 2014, por medio del cual se crea la Ley de transparencia y del derecho de acceso a la información Pública Nacional y se dictan otras disposiciones. 3. Anexo Manual de políticas de seguridad de la información, Política SGSI-A.8.2.2. 4. Declaración de Aplicabilidad Sistema de Gestión de Seguridad de la Información de fecha 12/12/2018, numeral A.8.2.2. 5. MIPG7^a. DIMENSIÓN- Componentes: Información y Comunicación y Actividades de Control.
Evidencia objetiva:	Una vez verificada la clasificación de la información establecida por el Instituto de Medicina Legal y Ciencias Forenses, se evidencia que a la fecha no hay definido lineamientos para el etiquetado y manejo de la información, de acuerdo al esquema de clasificación de la información; asimismo, no se evidenció en los documentos físicos, ni digitales, el etiquetado de la clasificación, tales como: Información Pública, Información Clasificada, Información Pública Clasificada e Información Pública Reservada. De igual forma, se evidencia que el informe pericial tiene dos (2) tipos de clasificaciones: Información Pública Clasificada e Información Pública Reservada, pero no se delimita a que informe pericial se le aplica una de estas.

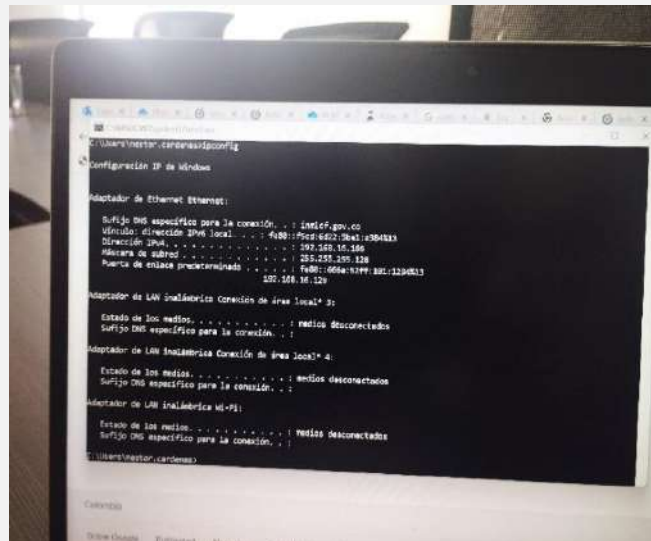
NO CONFORMIDAD No. 11	
Descripción:	El INMLCF no controla ni limita el acceso a la información, navegación e instalaciones, tanto físicos como lógicos; igualmente, para los servicios en la red, no determina el nivel de acceso al mismo (Filtrado Web) de manera apropiada, con las respectivas restricciones y perfiles específicos para cada cargo o función en los funcionarios de la entidad, con base en los requisitos del negocio y de seguridad de la información
Requisito aplicable:	1. NTC-ISO/IEC 27001:2013. Tecnología de la información. Técnicas de seguridad. Sistemas de Gestión de la Seguridad de la Información. Requisitos. Anexo A “Objetivos de control y controles de referencia”, A.9.1.1. “Política control de acceso” y A.9.1.2. “Acceso a redes y servicios de red”. 2. Instructivo Gestión de Acceso (DG-A-I-057), versión 2. 3. Instructivo control de acceso a las áreas restringidas del Instituto Nacional de Medicina Legal y Ciencias forenses (DG- M-I-115) versión 3. 4. Anexo Manual de políticas de seguridad de la información, Política SGSI-A.9.1.1 y Política SGSI-A.9.1.2.

5. Declaración de Aplicabilidad Sistema de Gestión de Seguridad de la Información de fecha 12/12/2018, numeral A.9.1.1.
6. MIPG7^a. DIMENSIÓN- Componente Actividades de Control

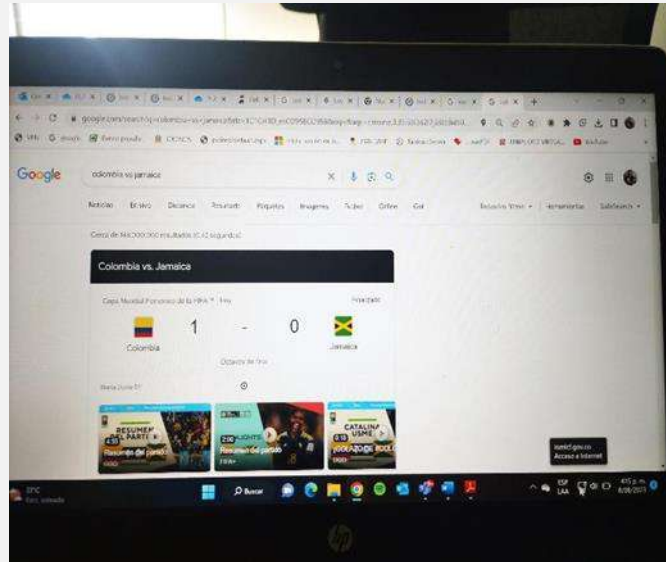
Durante la ejecución de la auditoria, se toma como evidencia el punto de red ubicado en la sala de juntas del sexto piso, donde se conecta un computador portátil de marca HP con serie 5CD107QBFP el cual no pertenece al dominio del INMLCF, encontrando que no limita el acceso a la red, ni a los datos de la entidad, obteniendo navegación libre y acceso a páginas no autorizadas, toda vez que no son insumos a la labor de los funcionarios ni presentan autorización, encontrando lo siguiente:

- El segmento de red no está cerrado, permitiendo que cualquier dispositivo se conecte y obtenga una asignación de Dirección IP dentro del DHCP, sin importar que no pertenezca al dominio inmlcf.gov.co.
- No hay coherencia entre los derechos de acceso y las políticas de limitación a los servicios de red.

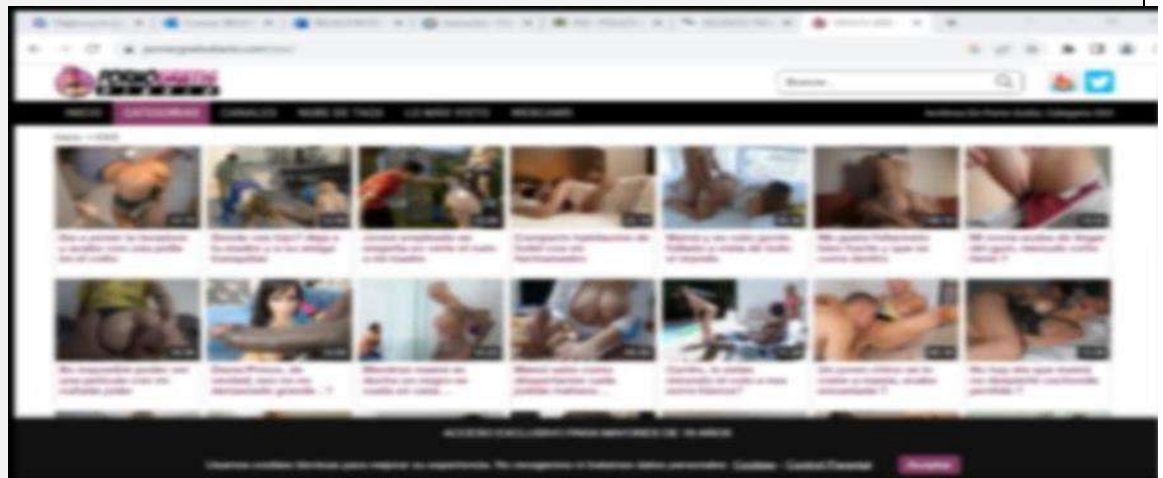
Evidencia objetiva:



Configuración IP asignada por el DHCP



Navegación realizada 08/08/2023 a las 16:15hrs



Navegación realizada, ingreso a páginas no autorizadas 08/08/2023 a las 16:16hrs

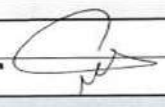
De igual manera, no está habilitado el registro de la huella en el control de ingreso y salida de funcionarios, contratistas y demás personal a las instalaciones del instituto, para prevenir el acceso físico no autorizado a las instalaciones y áreas de procesamiento de información de la organización.



Ingreso a las instalaciones del INMLCF Sede Central

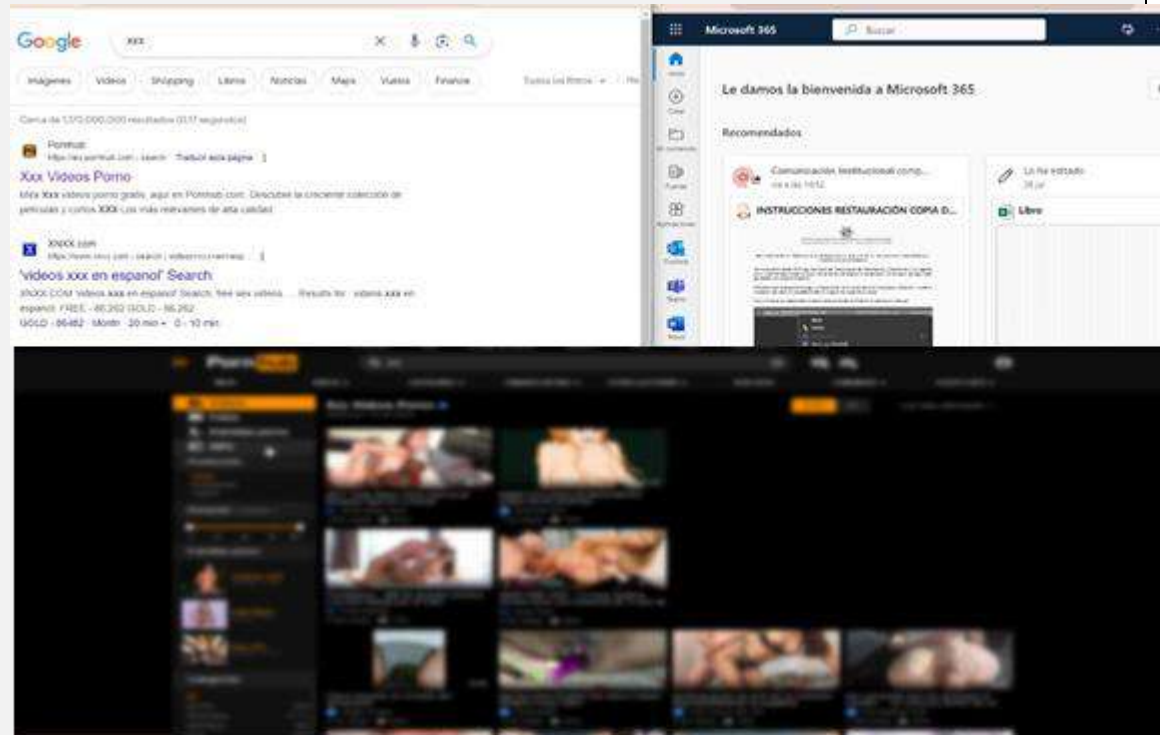
Para el control de acceso a redes se emplearon dos (2) estaciones de trabajo ubicadas en el quinto y sexto piso, en los cuales se realizó prueba de navegación a páginas de acceso para adultos mediante los computadores de serie MLX45018MR y serie 3CM1032KDK.

Por otro lado, se solicitó el día lunes 14/08/2023 de forma verbal y el día miércoles 16/08/2023 vía correo electrónico, al Grupo Nacional de Tecnologías de la Información y Desarrollo del Instituto Nacional de Medicina Legal y Ciencias Forenses, el listado de los funcionarios que tienen permiso de navegación abierta. Sin embargo, los soportes o formatos "SOLICITUD ACCESO A PAGINA WEB BLOQUEADA" donde fue autorizada la navegación libre para los funcionarios Angélica María Chica Badel y Miguel Arturo Velásquez Acevedo no fueron allegados ni cargados en la carpeta compartida "PLAN AUDITORIA INTERNA IA-08-2023". Por tal razón, se solicitó a la Dirección del Instituto estos soportes, donde se verificó que mediante correo electrónico del 06 de septiembre de 2022, la Dirección autoriza acceso a página web bloqueada específica "YOU TUBE" de la funcionaria Angélica María Chica Badel para participar en eventos con entidades externas. En relación al funcionario Miguel Arturo Velásquez Acevedo la Dirección manifestó que para este funcionario no existe solicitud de autorización de navegación libre.

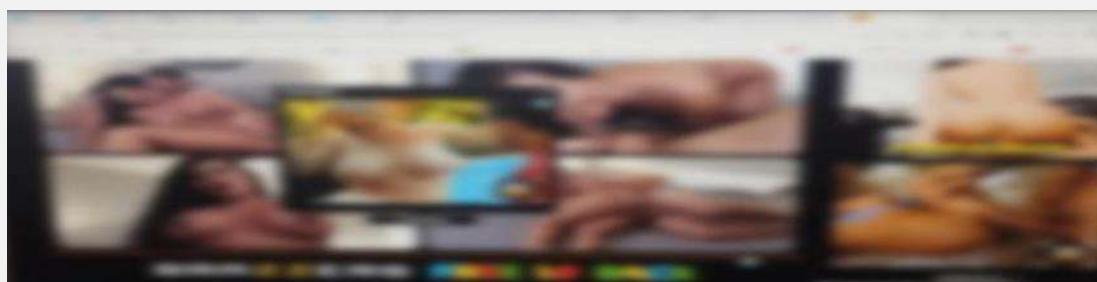
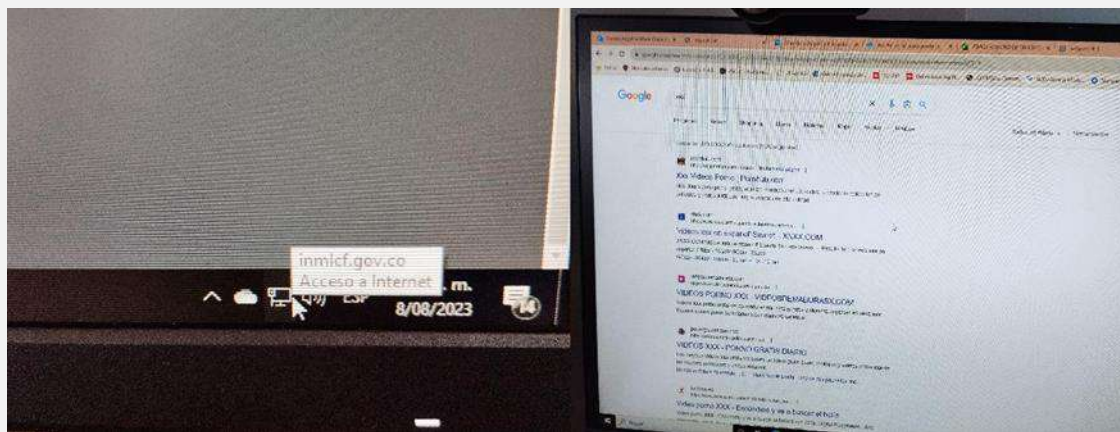
INSTITUTO NACIONAL DE MEDICINA LEGAL Y CIENCIAS FORENSES		
SOLICITUD ACCESO A PAGINA WEB BLOQUEADA		Código del formato: DG-A-I-057-F-004 Versión: 02 Página 1 de 1
INFORMACIÓN GENERAL INMLCF		
Fecha de solicitud: 2022-09-05	Unidad Organizacional: Dirección General	Firma: 
Nombre Coordinador o Jefe de la Unidad Organizacional: Jorge Arturo Jiménez Rojas		
INFORMACIÓN DE LOS ACCESOS SOLICITADOS		
Url, Detalle páginas, contenido	Justificación	Usuario autorizado
YouTube	Asistir a las reuniones programadas por entidades externas.	Marta Lucia Rodriguez Lardino
YouTube	Participar en eventos de entidades externas, información de temas administrativos.	Angelica Maria Chica Bodel
Acceso autorizado		
Permanente ☒	Elemento donde se aplicó el cambio:	
Temporal ☐	Especio Exclusivo para TIC	

Formato “SOLICITUD ACCESO A PAGINA WEB BLOQUEADA” con Acceso autorizado permanente a YouTube del 2022/09/05.

Muestra realizada de navegación libre:



Equipo de cómputo (quinto piso)



Equipo de cómputo (sexto piso)

NO CONFORMIDAD No. 12

Descripción:

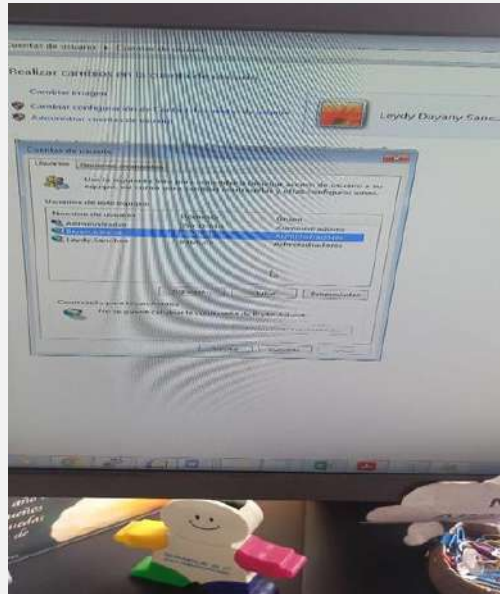
El INMLCF no asegura que las responsabilidades y la asignación de roles en los diferentes sistemas de información sean pertinentes y acordes a los controles de la norma y funciones que desempeña cada funcionario.

Requisito aplicable:

NTC-ISO/IEC 27001:2013. Tecnología de la información. Técnicas de seguridad. Sistemas de Gestión de la Seguridad de la Información. Requisitos. Control A.6.1.1. Anexo manual de políticas de seguridad de la información, A.6.1.1. Declaración de Aplicabilidad Sistema de Gestión de Seguridad de la Información de fecha 12/12/2018, A.6.1.1. MIPG7^a. DIMENSIÓN- Componente Actividades de Control.

Evidencia objetiva:

Dentro de la verificación realizada al SIAF se evidencia que el equipo de cómputo que tiene asignado la funcionaria LADY DAYANA SANCHEZ, administradora de nómina este cuenta con usuario administrador, software no licenciado de acceso remoto (Any Desk) y se evidencia que el equipo tiene un aviso donde anuncia que no se puede apagar.



Igualmente, la funcionaria, utiliza el programa o módulo solo para consultar, pero revisando en el sistema de información tienen habilitado todos los permisos tal cual lo muestra el reporte dado por el administrador funcional del SIAF

Imancera	PER - LADY NIYIRETH MANCERA R.	per_dnom	Datos de Nomina	X	X	X	X
----------	--------------------------------	----------	-----------------	---	---	---	---

La funcionaria el programa o módulo solo para consultar, pero revisando en el sistema de información tienen habilitado todos los permisos tal cual lo muestra el reporte dado por el administrador funcional del SIAF

Isanchez	PER-LEYDY DAYANY SANCHEZ	per_educ	Educacion formal de los funcionarios.	X	X	X	X
----------	--------------------------	----------	---------------------------------------	---	---	---	---

Este módulo solo lo consulta pero tiene todos los permisos según el reporte

Isanchez	PER-LEYDY DAYANY SANCHEZ	per_extr	Manejo de horas extras por fecha y tipo.	X	X	X	X
Isanchez	PER-LEYDY DAYANY SANCHEZ	per_afec	PARAMETRIZACION AFECTACION EMBARGOS	X	X	-	-
Isanchez	PER-LEYDY DAYANY SANCHEZ	per_amon	Amonestaciones y Comisiones	X	X	X	X
Isanchez	PER-LEYDY DAYANY SANCHEZ	per_bape	Manejo de la informacion de los bancos.	X	X	X	X
Isanchez	PER-LEYDY DAYANY SANCHEZ	per_cers	Certificado de tiempo y asignacion basic	X	X	X	X

No utiliza los siguientes módulos, pero tiene todos los permisos

Isanchez	PER-LEYDY DAYANY SANCHEZ	per_emb	Listado de Embargos y Generacion plano	X	X	X	X
----------	--------------------------	---------	--	---	---	---	---



La funcionaria manifiesta que este módulo lo maneja tesorería, pero ella tiene permisos sobre el mismo.

El funcionario CARLOS ALBERTO SAAVEDRA DELGADILLO, según sus funciones, no debe utilizar el programa o módulo que se relaciona a continuación, pero tiene todos los permisos sobre el mismo.

csaavedr	PER - CARLOS ALBERTO SAAVEDRA DELGADILLO	per_pago	Pagos segun fecha y tipo de novedad.	x	x	x	x
----------	--	----------	--------------------------------------	---	---	---	---

La funcionaria DALIDA GARCIA CHAVEZ, Utiliza el programa o módulo solo para REGISTRAR, pero revisando en el sistema de información tienen habilitado todos los permisos tal cual lo muestra el reporte dado por el administrador funcional del SIAF

dagarcia	PER - DALIDA GARCIA CHAVEZ	per_pago	Pagos segun fecha y tipo de novedad.	x	x	x	x
----------	----------------------------	----------	--------------------------------------	---	---	---	---

NO CONFORMIDAD No. 13**Descripción:**

El INMLCF no establece los controles necesarios para evitar la instalación de software no licenciado en los equipos corporativos de la entidad, sin considerar las implicaciones de depender de un software sin soporte.

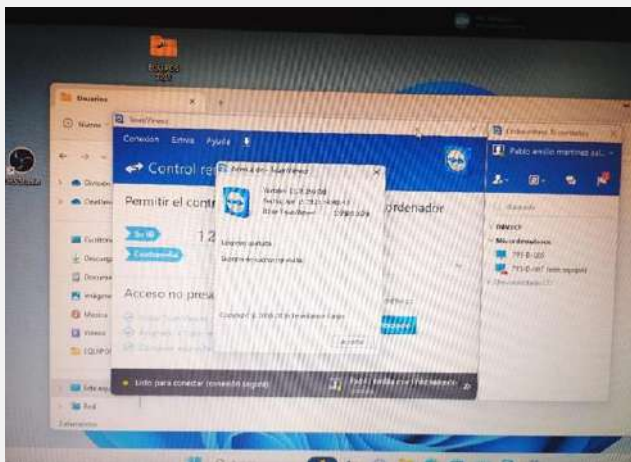
Requisito aplicable:

1. Ley 23 del 28 de enero 1982 "Sobre derechos de autor"
2. Ley 44 del 05 de febrero de 1993 "Por la cual se modifica y adiciona la Ley 23 de 1982..."
3. Ley 1915 de 2018 "Por la cual se modifica la Ley 23 de 1982 y se establecen otras disposiciones en materia de derecho de autor y derechos conexos."
4. Decreto 1474 del 15 de julio de 2002 "Por el cual se promulga el "Tratado de la OMPI, Organización Mundial de la Propiedad Intelectual, sobre Derechos de Autor (WCT)", adoptado en Ginebra, el veinte (20) de diciembre de mil novecientos noventa y seis (1996)"
5. Directiva Presidencial 01 del 25/02/1999 "Respeto al derecho de autor y a los derechos conexos"
6. Directiva Presidencial 02 del 12/02/2002 "Respeto al derecho de autor y los derechos conexos, en lo referente a utilización de programas de ordenador (software)"
7. Circular Nro. 17 del 01/06/2011 de la Unidad Administrativa Especial Dirección Nacional de Derecho de Autor "Modificación circular 12 del 2 de febrero de 2007, sobre recomendaciones, seguimiento y resultados sobre el cumplimiento de las normas en materia de derecho de autor sobre programas de computador (software)"
8. Circular Nro. 07 del 28 de diciembre de 2005 del Departamento Administrativo de la Función Pública "Verificación cumplimiento normas uso de software"
9. Decisión 351 de 1993 Comunidad Andina "Régimen común sobre derecho de autor y derechos conexos"

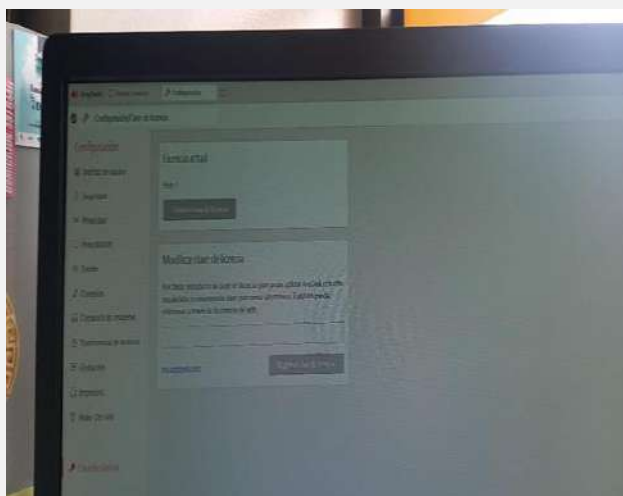


10. NTC-ISO/IEC 27001:2013. Tecnología de la información. Técnicas de seguridad. Sistemas de Gestión de la Seguridad de la Información. Requisitos, control A.12.5.1 y A.18.1.2
11. Anexo Manual de políticas de seguridad de la información, control A.12.5.1 y A.18.1.2
12. Declaración de Aplicabilidad Sistema de Gestión de Seguridad de la Información de fecha 12/12/2018, control A.12.5.1 y A.18.1.2
13. MIPG7ª. DIMENSIÓN- Componente Actividades de Control.

Se toma como muestra dos estaciones de trabajo encontrando en cada uno, software instalado de acceso remoto a los equipos de cómputo de diferentes proveedores como Any Desk y TeamViewer sin el respectivo licenciamiento.



Evidencia objetiva:





NO CONFORMIDAD No. 14

Descripción:

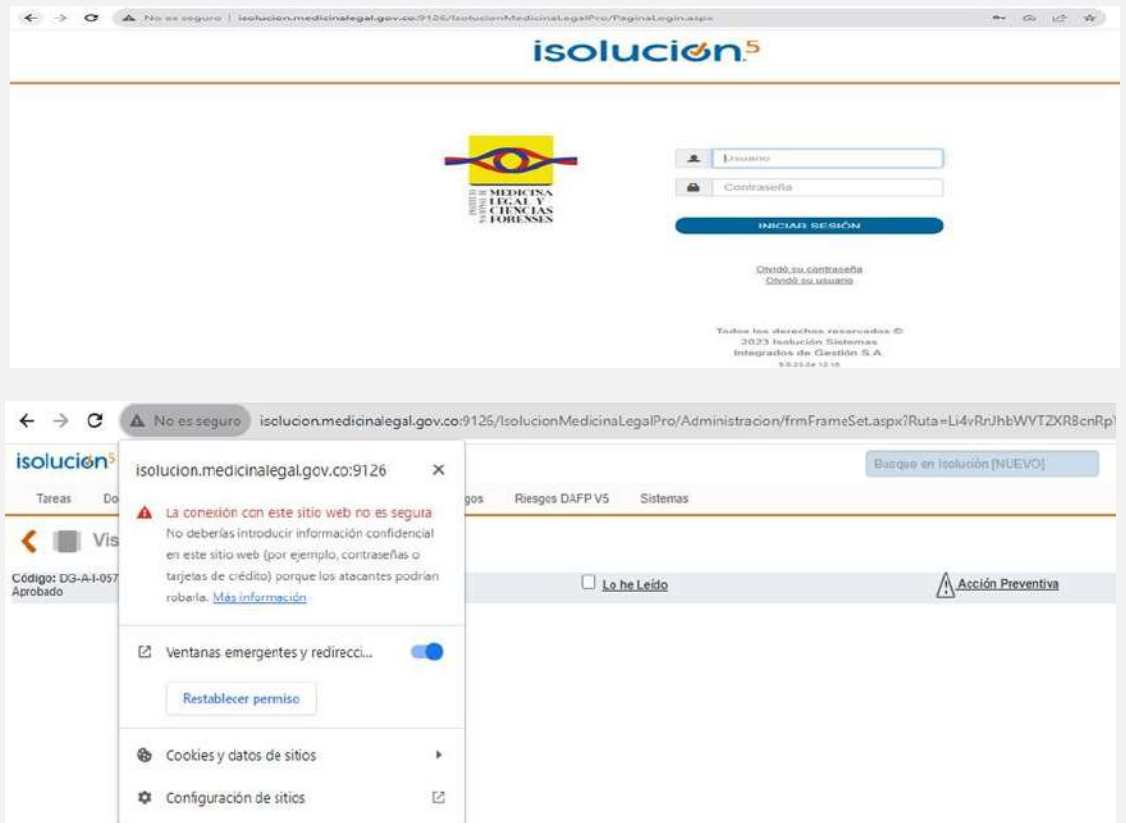
El INMLCF no establece los controles necesarios para cifrar las comunicaciones en los sistemas de información durante su ciclo de vida especialmente los que prestan servicios sobre las redes públicas.

Requisito aplicable:

1. NTC-ISO/IEC 27001:2013. Tecnología de la información. Técnicas de seguridad. Sistemas de Gestión de la Seguridad de la Información. Requisitos. Control A.14.1.3
2. Anexo Manual de políticas de seguridad de la información, A.14.1.3
3. Declaración de Aplicabilidad Sistema de Gestión de Seguridad de la Información de fecha 12/12/2018, Política A.14.1.3
4. MIPG7^a. DIMENSIÓN- Componente Actividades de Control.

Evidencia objetiva:

El sistema de información ISOLUCION, no cuenta con el certificado SSL



**NO CONFORMIDAD No. 15**

Descripción:	El Instituto Nacional de Medicina Legal y Ciencias Forenses, no cumple con lo establecido en el control A17.1. de la Norma de la NTC ISO 27001, gestión de continuidad de negocio facilitando el restablecimiento de las operaciones y de esta forma contrarrestar las interrupciones de las actividades misionales y de apoyo del INMLCF
Requisito aplicable:	1. NTC-ISO/IEC 27001:2013. Tecnología de la información. Técnicas de seguridad. Sistemas de Gestión de la Seguridad de la Información. Requisitos. anexo A “Objetivos de control y controles de referencia”, A.17. “ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTION DE CONTINUIDAD DEL NEGOCIO”. 2. Resolución No. 000837 del 22/11/2019, por la cual se adopta el Sistema de Gestión de la Seguridad de la Información- SGSI, la política de seguridad de la información y se establecen lineamientos para su uso y manejo, artículo 7 “revisión de la política de la seguridad de la información”; artículo 8 “roles y responsabilidades de los intervinientes en la organización de la seguridad de la información”, literal 3 “Comité de gobierno digital”. 3. MIPG7^a. DIMENSIÓN- Componentes Actividades de Control
Evidencia objetiva:	En el marco de la revisión de la implementación y seguimiento a la norma técnica de calidad ISO 27001, y de cara a la aplicación del control A 17 ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE CONTINUIDAD DEL NEGOCIO” dentro del INMLCF, se evidenció que el Instituto no tiene contemplado dentro de la continuidad del negocio un plan operativo que les permita la recuperación ante desastres, colapso de infraestructuras o situaciones de crisis, la puesta en funcionamiento de la operación de los procesos misionales y de soportes, si bien es claro que el respaldo información crítica del Instituto se encuentran en un sitio alterno, no se evidenció la documentación de los planes de continuidad que se establecieron para evitar y garantizar que los procesos comerciales críticos sigan funcionando en caso de daños o emergencias.

NO CONFORMIDAD No. 16

Descripción:	El Grupo Nacional de Tecnologías de la información y Desarrollo del Instituto Nacional de Medicina Legal y Ciencias Forenses, no garantiza que los funcionarios de la entidad, y en donde sea pertinente, los contratistas, tomen conciencia de las responsabilidades en seguridad de la información, al no dar cumplimiento a las actividades del plan de sensibilización en seguridad de la información de la vigencia 2022
Requisito aplicable:	1. NTC-ISO/IEC 27001:2013. Tecnología de la información. Técnicas de seguridad. Sistemas de Gestión de la Seguridad de la Información. Requisitos, numeral 7.3. “toma de conciencia”; anexo A “Objetivos de control y controles de referencia”, A.7.2.2 “toma de conciencia, educación y formación en la seguridad de la información.



	2. Anexo Manual de políticas de seguridad de la información, política SGSI A.7.2.2 3. Declaración de Aplicabilidad Sistema de Gestión de Seguridad de la Información de fecha 12/12/2018, A.7.2.2 “toma de conciencia, educación y formación en la seguridad de la información. 4. MIPG7^a. DIMENSIÓN- Componente Actividades de Control.
Evidencia objetiva:	Una vez revisada la Declaración de Aplicabilidad del Sistema de Seguridad de la Información del Instituto Nacional de Medicina Legal y Ciencias Forenses, ubicada en la carpeta compartida “PLAN AUDITORIA INTERNA AI-08-2023” asignada por el instituto para el cargue de los soportes de auditoria mediante archivo en formato Excel denominado “Declaracion_Aplicabilidad-v1-2019_01-28 (2)”, se observa en el control A.7.2.2. Que el Instituto estableció un plan de apropiación del SGSI, sin embargo, los soportes de la ejecución del mismo no fueron presentados ni cargados en la carpeta compartida. De igual forma, se verifica los lineamientos establecidos en la política SGSI A.7.2.2. que se registra en el documento denominado “anexo manual de políticas de seguridad de la información”, la cual está en el sistema de información ISOLUCION y establece que “el Grupo Nacional de Tecnologías de Información y Desarrollo debe definir un programa de sensibilización de seguridad de la información, incluyendo el proceso de evaluación, dirigido a los funcionarios, contratista o terceros que tengan relación con los activos de información del Instituto”, de lo cual, se evidencia el plan de sensibilización en seguridad de la información de fecha 2022/01/09, sus directrices y cronograma para la realización de las diferentes actividades, sin sus respectivos soportes. El cronograma para la vigencia 2022 fue el siguiente:

10. Cronograma de Actividades

Tipo	Actividad	Usuarios	Medio de difusión	Tema	2022											
					E	F	M	A	M	J	J	A	S	O	N	D
Campañas	Charla	Central	Video Conferencia	Conocimiento general del sistema de gestión de seguridad							X					
Campañas	Charla	Central	Video Conferencia	Conocimiento de las políticas de seguridad de la información												X
Campañas	Infografía	Central	correo/intranet / protector pantalla	Respuesta al incidente: ¿a quién contacto? "¿Qué debo hacer?"					X							
Campañas	Infografía	Central	correo/intranet / protector pantalla	Seguridad de escritorio: sobre el uso de protectores de pantalla, restringiendo la vista de los visitantes a la información en pantalla						X						
Campañas	Infografía	Central	correo/intranet / protector pantalla	Uso y administración de la contraseña, incluye la creación, la frecuencia de los cambios y la protección.							X					
Campañas	Infografía	Central	correo/intranet / protector pantalla	Protección contra virus, gusanos, caballos de troya y otros códigos maliciosos – Enfoque 1								X				
Campañas	Infografía	Central	correo/intranet / protector pantalla	Protección contra virus, gusanos, caballos de troya y otros códigos maliciosos – Enfoque 2									X			
Campañas	Infografía	Central	correo/intranet / protector pantalla	Uso apropiado de internet										X		
Campañas	Infografía	Central	correo/intranet / protector pantalla	Ingeniería social											X	

Mediante correo electrónico de fecha 2023/08/11, se solicita al Grupo Nacional de Tecnologías de la Información y Desarrollo, los soportes de cumplimiento al cronograma establecido en el numeral 10, del plan de sensibilización en seguridad de la información y los soportes de la estrategia de seguimiento e informes de los resultados de medición de la efectividad del programa o plan de sensibilización, según lo registrado en el numeral 7.3 y 7.4 del documento en mención, para lo cual, a la fecha no han dado respuesta del mismo, evidenciando el incumplimiento del programa y de las actividades de monitoreo y efectividad del mismo, dentro de las que se debieron haber empleado para evaluar las campañas de sensibilización, siendo las siguientes:

- Evaluaciones o cuestionarios.
- Uso de observadores independientes o auditores, que evalúan la efectividad del programa.
- Verificación de la cantidad de incidentes abiertos y su causa.
- Ataques de ingeniería social, posteriores a las sensibilizaciones.

**NO CONFORMIDAD No. 17**

Descripción:	El INMLCF no define adecuadamente los protocolos para llevar a cabo las operaciones de comunicación y minimizar la probabilidad de ocurrencia de comprometer la seguridad de la información de la entidad contra la pérdida o alteración de la misma
Requisito aplicable:	1. NTC-ISO/IEC 27001:2013. Tecnología de la información. Técnicas de seguridad. Sistemas de Gestión de la Seguridad de la Información. Requisitos. anexo A “Objetivos de control y controles de referencia A.12.1.1 Procedimientos de operación documentados. 2. Resolución No. 000837 del 22/11/2019, por la cual se adopta el Sistema de Gestión de la Seguridad de la Información- SGSI, la política de seguridad de la información y se establecen lineamientos para su uso y manejo. 3. MIPG7^a. DIMENSIÓN- Componentes: Actividades de Control y Actividades de Control.
Evidencia objetiva:	El INMLCF cuenta con una hiper convergencia que le permite tener copia de respaldo de sus sistemas críticos, sin embargo, se evidencia que algunos funcionarios cuentan con disco duros externos en los cuales realizan copias de respaldo adicionales y estos no cuentan con ningún tipo de seguridad física ni lógica, no se encuentra documentado, exponiendo a posibles materializaciones del riesgo de la información

NO CONFORMIDAD No. 18

Descripción:	El INMLCF no implementa los controles criptográficos necesarios con el objetivo de prevenir el acceso no autorizado a la información en caso de pérdida de activos que la contengan tales como computadores, memorias USB, etc.
Requisito aplicable:	1. NTC-ISO/IEC 27001:2013. Tecnología de la información. Técnicas de seguridad. Sistemas de Gestión de la Seguridad de la Información. Requisitos. Anexo A “Objetivos de control y controles de referencia”, control A.8.3.1 Gestión de medios de soporte removibles y A.18.1.5 Reglamentación de controles criptográficos 2. Anexo manual de políticas de seguridad de la información, Política SGSI - A.8.3.1 y A.18.1.5. 3. Matriz declaración de Aplicabilidad Sistema de Gestión de Seguridad de la Información de fecha 12/12/2018, A.8.3.1 y A.18.1.5.

**4. MIPG7^a. DIMENSIÓN- Componente Actividades de Control.****Evidencia objetiva:**

Los equipos de cómputo de la entidad no cuentan con el control de seguridad necesario para la seguridad de las operaciones permitiendo la acción de PRINT SCREEN, lectura y escritura de CD/DVD y USB y otros dispositivos de almacenamiento, utilizados y no están protegidos contra daño, pérdida o hurto, con el propósito de evitar acceso no autorizado a la información gestionada en ellos.

NO CONFORMIDAD No. 19**Descripción:**

El INMLCF no previene el aprovechamiento de las vulnerabilidades técnicas al no subsanar las debilidades encontradas en las plataformas tecnológicas del SIAF y SIAF BD

Requisito aplicable:

1. NTC-ISO/IEC 27001:2013. Tecnología de la información. Técnicas de seguridad. Sistemas de Gestión de la Seguridad de la Información. Requisitos. Anexo A “objetivos de control y controles de referencia” A.12.6.1 “Gestión de las vulnerabilidades técnicas”.
2. Matriz Declaración de Aplicabilidad Sistema de Gestión de Seguridad de la Información de fecha 12/12/2018, A.12.6.1 “Gestión de las vulnerabilidades técnicas”.
3. Anexo Manual de políticas de seguridad de la información, Política A.12.6.1.
4. MIPG7^a. DIMENSIÓN- Componente Actividades de Control.

Evidencia objetiva:

Teniendo en cuenta el documento “Análisis de Vulnerabilidades y Pruebas de Penetración” a la Plataforma de Tecnologías de la Información del INMLCF, practicada en diciembre del 2022, y tomando como muestra los servidores SIAF (192.168.0.84) y SIAF BD (192.168.0.148), se identificó que el Instituto obtuvo información de las vulnerabilidades técnicas y evaluó la exposición de la organización a estas vulnerabilidades, sin embargo, no tomó las medidas apropiadas para tratar el riesgo al no ejecutar un plan de remediación o plan de acción correctiva para subsanar las vulnerabilidades señaladas en el análisis en mención, tomar las medidas apropiadas para prevenir su aprovechamiento y asegurar la integridad de estos sistemas.

NO CONFORMIDAD No. 20**Descripción:**

El INMLCF no tiene procedimiento para realizar el borrado seguro para los equipos que contienen medios de almacenamiento



Requisito aplicable:	1. NTC-ISO/IEC 27001:2013. Tecnología de la información. Técnicas de seguridad. Sistemas de Gestión de la Seguridad de la Información. Requisitos. Anexo A “objetivos de control y controles de referencia” A.11.2.7 “Disposición Segura o reutilización de equipos”. 2. Matriz Declaración de Aplicabilidad Sistema de Gestión de Seguridad de la Información de fecha 12/12/2018, A.11.2.7 “Disposición Segura o reutilización de equipos” 3. Anexo Manual de políticas de seguridad de la información, Política A.11.2. 4. MIPG7^a. DIMENSIÓN- Componentes: Actividades de Control y Actividades de Control.
Evidencia objetiva:	Verificada la herramienta ISOLUCION sobre el procedimiento establecido por el INMLCF para el borrado seguro de los equipos que contienen medios de almacenamiento, se identificó que el Instituto no cuenta con un procedimiento establecido para realizar la disposición segura o reutilización de los equipos y de esta manera asegurar que cualquier dato confidencial o software licenciado haya sido retirado o sobrescrito en forma segura antes de su disposición final o reuso.

NO CONFORMIDAD No. 21

Descripción:	El Grupo Nacional de Tecnologías de la información y Desarrollo, no facilito el suministro de parte de la información solicitada de forma verbal y correo electrónico, durante el ejercicio de la auditoria.
Requisito aplicable:	1. NTC-ISO/IEC 27001:2013. Tecnología de la información. Técnicas de seguridad. Sistemas de Gestión de la Seguridad de la Información. Requisitos, numeral 7.5.3 “control de la información documentada”, literal a). 2. Decreto Ley 403 del 16/03/2020, “por la cual se dictan normas para la correcta implementación del acto legislativo 04 de 2019 y el fortalecimiento del control fiscal, artículo 151. 3. MIPG7^a. DIMENSIÓN- Componentes: Información y Comunicación y Actividades de Control.
Evidencia objetiva:	El Grupo Nacional de Tecnologías de la información y Desarrollo del INMLCF , no dio respuesta del suministro de la información requerida durante la ejecución de la misma, toda vez, que en dos (2) oportunidades se solicitó mediante correo electrónico, los soportes que evidenciaran el cumplimiento al cronograma del plan de sensibilización y seguimiento para la vigencia 2022 (Registro 1) y a la fecha no se ha obtenido respuesta alguna; asimismo, se solicitó el listado de los funcionarios que tienen navegación



abierta y los soportes de solicitud de acceso a página web bloqueada (DG-A-I-057-F-004) de dos **funcionarios** de la entidad previa autorización del jefe de la unidad (Registro 2), sin recibir respuesta alguna; de igual forma, no fue compartida esta información en la carpeta asignada para tal fin, durante el proceso de auditoría. Lo anterior, incumpliendo la norma NTC-ISO/IEC 17025:2013 y la Ley 403 de 2020, que en su artículo 151, dice:

“... ARTÍCULO 151. DEBER DE ENTREGA DE INFORMACIÓN PARA EL EJERCICIO DE LAS FUNCIONES DE LA

UNIDAD U OFICINA DE CONTROL INTERNO. Los servidores responsables de la información requerida por la unidad u oficina de control interno deberán facilitar el acceso y el suministro de información confiable y oportuna para el debido ejercicio de sus funciones, salvo las excepciones establecidas en la ley. Los requerimientos de información deberán hacerse con la debida anticipación a fin de garantizar la oportunidad y completitud de la misma.

El incumplimiento reiterado al suministro de la información solicitada por la unidad u oficina de control interno dará lugar a las respectivas investigaciones disciplinarias por la autoridad competente...”

Reiterando solicitud para auditoria interna

HUGO ALONSO PEREZ CARVAJAL <alonso.perez1689@correo.policia.gov.co>

Lun 14/08/2023 7:19

Para:dinformatica@medicinalegal.gov.co <dinformatica@medicinalegal.gov.co>;Sonia Patricia Castañeda Neira <sonia.castaneda@medicinalegal.gov.co>

Buenos días.

Cordial saludo,

Ingeniera

SONIA PATRICIA CASTAÑEDA NEIRA

Coordinadora Grupo Nacional de Infraestructura Tecnológica y Servicios Informáticos
Instituto Nacional de Medicina Legal y Ciencias Forenses
Ciudad

En atención a que el día viernes 11 de agosto de 2023, siendo las 08:57 a.m, se solicitó la información relacionada en el presente correo, respetuosamente, me permito solicitar que está, sea allegada con **plazo hoy lunes 14/08/2023 a las 10:00 a.m**, así:

- De acuerdo con el tratamiento dado a la auditoria AI-20-2022 y en el ejercicio interno de identificar las posibles causas que generaron la no conformidad, al realizarlo conforme al Procedimiento de acciones vigente, teniendo en cuenta que las metodologías para el análisis de causas adoptadas institucionalmente, son la espina de pescado y los por qué; solicitamos los soportes construidos entre otros el formato de Acta de Reunión establecida en el instructivo DG-E-I-005 versión vigente.
- Asimismo, de acuerdo al documento **“PLAN DE SENSIBILIZACIÓN EN SEGURIDAD DE LA INFORMACIÓN”** del 09 de enero de 2022, donde se establece en el numeral 10 el cronograma de actividades, respetuosamente solicitamos los soportes correspondientes al cumplimiento del cronograma en mención.
- De igual forma, solicitamos adjuntar los soportes de la estrategia de seguimiento e informes de los resultados de medición de la efectividad del programa o plan de sensibilización, según lo registrado en el numeral 7.3 y 7.4 del documento en mención.
- Igualmente, solicito adjuntar en la carpeta Revisión por la Dirección, la información para la Revisión por la Alta Dirección correspondiente a la vigencia 2022 realizada en la presente vigencia, la cual fue allegada por el Grupo Nacional de Tecnologías de la Información y Desarrollo a la oficina de planeación, previa solicitud de esta, lo anterior, teniendo en cuenta que según la actividad No. 1 “preparar la información para la revisión del sistema integrado de gestión por la alta dirección” del numeral 7.4.1 del documento DG-E-P-003, establece que la oficina de planeación debe realizar la solicitud en el mes de diciembre.

Por lo anteriormente expuesto, solicitamos que estos soportes sean cargados en la carpeta compartida según evidencia, para tener claridad a que refiere los documentos, así:



Registro No. 1

Solicitud información auditoria interna

HUGO ALONSO PEREZ CARVAJAL <alonso.perez1689@correo.policia.gov.co>

Miércoles 16/08/2023 7:51

Para: División Informática - INMLCF - Sede Central <dinformatica@medicinalegal.gov.co>; Sonia Patricia Castañeda Neira <sonia.castaneda@medicinalegal.gov.co>

Cordial saludo,

Ingeniera

SONIA PATRICIA CASTAÑEDA NEIRA

Coordinadora Grupo Nacional de Infraestructura Tecnológica y Servicios Informáticos

Instituto Nacional de Medicina Legal y Ciencias Forenses

Ciudad

En atención a que el día lunes 14 de agosto de 2023, se solicitó el listado de los usuarios que actualmente tienen la navegación libre, soportes (formato) de solicitud de navegación libre para los funcionarios Dra. Angelica Chica y Dr. Velázquez y aun esta información no ha sido cargada en la carpeta compartida; respetuosamente, me permito recordar llegar la información solicitada con **plazo hoy miércoles 16 de agosto de 2023 a las 10:00 a.m.**

Agradeciendo la atención prestada y su pronta respuesta.

Registro No. 2

NO CONFORMIDAD No. 22

Descripción:

El proceso de Gestión de Infraestructura Tecnológica y Servicios Informáticos y el Sistema de Gestión de Seguridad de la Información, no establece la identificación de todos los riesgos mencionados en la norma NTC-ISO/IEC 17025:2013, con el fin de prevenir o reducir efectos indeseados, logrando la mejora continua

Requisito aplicable:

1. NTC-ISO/IEC 27001:2013. Tecnología de la información. Técnicas de seguridad. Sistemas de Gestión de la Seguridad de la Información. Requisitos, numeral 6.1. "acciones para tratar riesgos y oportunidades".
2. Anexo manual de políticas de seguridad de la información, Política SGSI-A.6.2.1, Política SGSI-A.11.2.1, Política SGSI-A.12.1.4, Política SGSI-A.12.6.1, Política SGSI-A.15.1.1.
3. Matriz declaración de Aplicabilidad Sistema de Gestión de Seguridad de la Información de fecha 12/12/2018, A.6.2.1, A.11.2.1, A.12.1.4, A.12.6.1, A.15.1.1.
4. MIPG7^a. DIMENSIÓN- Componentes: Evaluación del Riesgo y Actividades de Control

Evidencia objetiva:

Una vez verificado el sistema de información ISOLUCION, se establece que el Grupo Nacional de Tecnología y Desarrollo, ha identificado cuatro (4) riesgos, así:

Riesgo de corrupción:

GITS-27“Posibilidad de entregar, manipular o alterar la información contenida en los sistemas de información el cual puede ser utilizado para beneficio propio o a un tercero”

Riesgo de seguridad de la información:

Riesgo GISTS-28 “Pérdida de Disponibilidad”, cuya descripción corresponde a: “Todas las unidades organizacionales a Nivel Nacional que están expuestas a la pérdida de disponibilidad en los servidores que soportan los sistemas de información institucionales, dañan la imagen o reputación del Instituto y pérdida de confianza por parte de las entidades y ciudadanos que usan los servicios del INMLCF, por causa del aprovechamiento de las vulnerabilidades de la plataforma tecnológica y debilidades en el aseguramiento de la misma.”

Riesgo de gestión:

GITS-29 “Posibilidad de afectación reputacional por vulnerar los activos de información debido al incumplimiento en la política de seguridad de la información”

GITS-30 “Posibilidad de afectación reputaciones por el manejo inadecuado del recurso informático debido al incumplimiento de los lineamientos, políticas, procesos y procedimientos establecidos”

Lo anterior, no garantiza el cumplimiento a los riesgos o controles mínimos que debe tener la organización para mitigar o controlar efectos no deseados, tales como:

- La entidad no identifica el riesgo de trabajar con dispositivos móviles en entornos no protegidos, toda vez que es importante el cuidado cuando se usan dispositivos móviles en lugares públicos, salas de reuniones y otras áreas no protegidas, como es el caso de lo evidenciado en el hallazgo No. 11, donde se toma como evidencia el punto de red ubicado en la sala de juntas del sexto piso y se conecta un computador portátil de marca HP con serie 5CD107QBFP el cual no pertenece al dominio del INMLCF, encontrando que no limita el acceso a la red, ni a los datos de la entidad, obteniendo navegación libre y acceso a páginas no autorizadas.
- La entidad no identifica el riesgo de amenazas y peligros del entorno, toda vez que es importante establecer que los puestos de trabajo donde se procese información que maneje datos sensibles se ubiquen cuidadosamente para reducir o minimizar el riesgo de que personas no autorizadas puedan ver la información durante su uso.

- Igualmente, se deben adoptar los controles necesarios para minimizar el riesgo de amenazas físicas y ambientales potenciales, por ejemplo: robo, incendio, explosivos, humo, agua, polvo, vibración, efectos químicos, interferencia en el suministro eléctrico, interferencia en las comunicaciones, radiación electromagnética y vandalismo.
- El INMLCF, no establece el riesgo de acceso o cambios no autorizados al ambiente de producción, toda vez que se debería separar los ambientes de desarrollo, prueba y producción para reducir este riesgo.
- La entidad no identificó o valoró el riesgo de vulnerabilidad técnica, toda vez que es importante definir y establecer los roles y responsabilidades asociados con la gestión de la vulnerabilidad técnica, incluido el seguimiento de la vulnerabilidad, la valoración del riesgo de vulnerabilidad, la colocación de parches, el seguimiento de activos y cualquier responsabilidad de coordinación requerida.
- El INMLCF, no identifica el riesgo asociado con el acceso de proveedores, toda vez que se hace necesario establecer requisitos de seguridad de la información para mitigar los riesgos asociados con el acceso de proveedores a los activos de la entidad.

OPORTUNIDADES DE MEJORA

SITUACIÓN ACTUAL	SITUACIÓN DESEADA
No. 01. El procedimiento gestión de acciones correctivas, acciones preventivas y acciones de mejora (DG-C-P-014) versión 13, en su actividad 2, tarea 8, nota 1, establece “el tratamiento a los hallazgos en auditoría interna es aprobado por el auditor líder de la Oficina de Control Interno”.	Estudiar la posibilidad de ajustar y modificar el procedimiento gestión de acciones correctivas, acciones preventivas y acciones de mejora (DG-C- P-014), donde se establezca la aprobación del tratamiento de los hallazgos en la auditoría interna por parte del responsable del proceso auditado, a fin de mantener la independencia y objetividad de la Oficina de Control Interno en su función de seguimiento y evaluación de la eficacia de las acciones tomadas.
No. 02. La Resolución No. 000837 del 22/11/2019, establece en su artículo 3, “cumplir las funciones establecidas por el comité de gobierno digital, para tratar temas estratégicos relacionados con seguridad de la información y proponer recomendaciones” y la Resolución 001123 del 12/12/2018, establece las funciones del comité de gobierno digital, cuyo objeto es garantizar la adecuada planeación,	Unificar criterios, responsabilidades y funciones en un comité que se enfoque para la gestión de la seguridad de la información y su implementación (es decir los objetivos de control, los controles, las políticas, los procesos y los procedimientos), revisión al cumplimiento en el procesamiento y procedimientos de información dentro de cada proceso, revisión anual de las políticas y normas de seguridad de

implementación y mantenimiento de la estrategia de Gobierno Digital, según los lineamientos establecidos por la MINTIC, siendo ambigua las dos resoluciones, la cual no garantizan el cumplimiento a la implementación del SGSI bajo los requisitos de la norma NTC-ISO/IEC 27001:2013.	la información, asegurando su conveniencia, adecuación y eficacia continua; o por el contrario, ampliar las funciones del comité de Gobierno digital
No. 03. El anexo “metodología para abordar la no conformidad, su análisis de causas, implementación y evaluación de eficacia (DG-C-P-014-AX- 004)” aborda solamente dos (2) metodologías que se pueden utilizar para realizar análisis de causas en la entidad “Porqué” y “Diagrama Causa – Efecto o Espina de Pescado”.	Estudiar la posibilidad de actualizar el presente anexo, ampliando las metodologías para análisis de causas, dentro de las que se encuentran, las siguientes: • Tabla de priorización. • Diagrama de Pareto. • Árbol de fallos. • Otras
No. 04. El documento “manual del sistema integrado de gestión (DG- MANUAL-001)” en su artículo 6.1 establece la Responsabilidad y Compromiso de la Dirección, mediante la articulación y alineación conjunta de los requisitos de las diferentes normas técnicas (NTC- ISO/IEC 17025:2017, NTC-ISO 9001:2015, NTC-ISO/IEC 17024:2013,NTC-ISO/IEC 27001:2013, NTC-ISO 14001:2015, NTC-ISO-IEC 17020:2012), Decreto 1072 de 2015 y Sistema de Control Interno séptima dimensión de MIPG	Fortalecer el documento “manual del sistema integrado de gestión (DG- MANUAL-001)”, incluyendo los literales del a) al h) establecidos en el numeral 5.1. liderazgo y compromiso de la norma NTC-ISO/IEC 27001:2013, donde se debe asegurar que la alta Dirección demuestre liderazgo y compromiso con respecto al sistema de gestión de la seguridad de la información
No. 05. Actualmente, el Grupo Nacional de Tecnología y Desarrollo, establece en el documento “Anexo Manual de Políticas de Seguridad de la Información” lineamientos para el cumplimiento a los diferentes controles de la norma, estos lineamientos no existen o, por el contrario, la responsabilidad se la trasladan a los demás procesos.	Ajustar el documento “Anexo Manual de Políticas de Seguridad de la Información”, generando lineamientos vigentes y aplicables a la organización en los 114 controles de la norma
• No. 06. El INMLCF, dentro de sus lineamientos institucionales posee un procedimiento de control de cambios, lo cual es válido para mantener la seguridad de la información, asimismo, según lo manifestado por los desarrolladores del Grupo Nacional de Tecnologías de la Información, ningún	Los procesos de cambio pueden conllevar riesgos asociados para la seguridad de la información, este análisis se debería adicionar dentro del procedimiento de gestión de cambios toda vez que no se evalúa. Otro elemento esencial es establecer en un ambiente de pruebas los cambios realizados

	cambio se desarrolla sin el aprobado de la Subdirección, a lo cual es un buen punto de control, sin embargo, dentro de su procedimiento está descrito que: Convocar al Comité de Cambios de ser necesario, de lo contrario dar continuidad requerimiento. El comité asesor de cambios será conformado cuando el cambio requerido cause un gran impacto en la prestación de los servicios institucionales o cuando sea requerido por necesidad del servicio Este comité sería un control mucho más fuerte.	antes de salir a producción y estos deben estar avalados por el dueño de la necesidad, lo cual no se encuentra descrito en el procedimiento. Finalmente, siempre se debe convocar al comité de gestión del cambio y mantener un registro (acta) que contenga al menos la información de: • Quien autoriza los cambios • Quien realiza los cambios • Fecha • Descripción de las tareas • Validación del cambio • Otros Dentro de este comité se debe exponer por parte del dueño de la necesidad el porqué del cambio y ser viabilizado por parte del grupo de T.I y por la subdirección como se viene haciendo en el momento
	• No. 07. Sistemas de información desarrollados en leguajes de programación con unos parámetros de seguridad de información mínimos	Migrar a unos sistemas de información actualizados, que les genere alertas en caso de que se identifique una mala práctica en la aplicación del mismo, de la misma forma que le permita generar unos reportes que sirvan para la toma de decisiones gerenciales y técnicas como, por ejemplo: Informes periciales: un software que genere alertas cuando algún funcionario no autorizado quiera realizar cambio a los informes o que intente visualizarlo sin los permisos. Nomina: un S.I que genere alertas en caso de detectar que se está causando alguna novedad de nómina a la cual el funcionario no tenga derecho. Entre otras

CONCLUSIONES DE LA AUDITORÍA

- El INMLCF presenta debilidades en el cumplimiento a la Norma Técnica Colombiana NTC -ISO/IEC 27001: 2013, toda vez que no garantiza la implementación de los controles y la operacionalización de la seguridad de la información, necesarios para mitigar los riesgos de manera apropiada en cada uno de los 114 controles adoptados por la entidad, con base en los requisitos del negocio y de seguridad de la información, estableciendo que los estándares de calidad, seguridad y buenas



prácticas, no son adecuados con el cumplimiento de los objetivos institucionales y propósito de la organización.

- El INMLCF adopta la política de seguridad de la información en la resolución No. 000837 de 22 de noviembre de 2019, pero no asegura que las políticas de seguridad de la información específicas sean adecuadas para el propósito de la organización, toda vez que no tiene definidas la política para Dispositivos Móviles, Política Control de Acceso, Política sobre el uso de Controles Criptográficos, Política de Escritorio limpio y pantalla limpia, Políticas y procedimientos de transferencia de la información, Política de Desarrollo Seguro y Política de Seguridad de la información para la relación con proveedores que brinden orientación y soporte, por parte de la dirección, para la seguridad de la información de acuerdo con los requisitos del negocio y con las leyes y reglamentos pertinentes, cuyo cumplimiento del Plan Estratégico de Tecnologías de la información y Comunicaciones (PETIC), no está articulado con la evaluación de las políticas de seguridad de la información.
- El INMLCF, no establece riesgos asociados a la confidencialidad e integridad de la información del aplicativo SIAF módulo nómina, toda vez que la entidad no aplica los controles establecidos en la norma NTC-ISO/IEC 27001:2013, cuyo resultado se encuentra relacionado en las no conformidades evidenciadas de la presente auditoría, que en principio, no existe una adecuada separación de deberes y responsabilidades entre los grupos y dependencias para evitar y reducir posibles modificaciones no autorizadas, intencionales o uso indebido de los activos de la entidad; lo cual, el tratamiento del riesgo “perdida de disponibilidad” no garantiza la integridad de la información en el sistema de información SIAF
- El Grupo Nacional de Tecnologías de la Información y Desarrollo del INMLCF, no aplica adecuadamente el análisis de causas para las no conformidades reales evidenciadas en el informe de auditoría interna AI-20-2022, conforme a las metodologías definidas por la entidad.
- Se verifica el tratamiento de riesgos establecidos por el Grupo Nacional de Tecnologías de la Información y Desarrollo del INMLCF, donde se establece que no son efectivos los controles de los riesgos asociados al proceso de Gestión de Infraestructura Tecnológica y Servicios Informáticos y el Sistema de Gestión de Seguridad de la Información, ni al sistema de información SIAF, entre otros, para lo cual, se requiere fortalecer los controles y analizar otros riesgos transversales a la entidad, fortaleciendo el sistema de seguridad de la información.
- Verificado el cumplimiento de los objetivos estratégicos relacionados con el proceso de Gestión de Infraestructura Tecnológica y Servicios Informáticos y el Sistema de Gestión de Seguridad de la Información, se establece que este fue cumplido conforme al objetivo estratégico “garantizar la disponibilidad de servicios de tecnologías de la información y comunicaciones”.

**FECHA DE
ELABORACIÓN**


Aprobado: Néstor Fan León Niño
Jefe Oficina de Control Interno

2023-10-30