



INSTITUTO NACIONAL DE MEDICINA LEGAL Y CIENCIAS FORENSES

INFORME EJECUTIVO DE AUDITORÍA

Página 1 de 6

ID DE LA AUDITORIA:	PROCESO A AUDITAR:	UNIDAD ORGANIZACIONAL:	FECHA DE AUDITORIA:
AI-16-2020	Gestión de la Infraestructura Tecnológica y Servicios Informáticos Y Sistema de la Seguridad de la Información	Grupo Nacional de Tecnologías de Información y Desarrollo (Sede Central) Dirección Regional Oriente Dirección Regional Bogotá	Planeación: 2020-11-03 al 2020-11-11 Ejecución: 2020-11-12 al 2020-11-20 Informe: 2020-11-23 al 2020-12-04

OBJETIVOS DE LA AUDITORÍA:

Verificar que las actividades desarrolladas que hacen parte del Subsistema de Seguridad de la Información, cumplan con los criterios de la auditoria con el fin de evaluar su adecuado funcionamiento, de manera que permita contribuir a la mejora continua del Sistema Integrado de Gestión, así como la efectividad de los controles existentes, evaluación de los riesgos atinentes, cumplimiento de sus indicadores y seguimiento a los planes de mejoramiento o acciones de mejora.

ALCANCE DE LA AUDITORIA:

Desde la última fecha de auditoría realizada incluido hasta la fecha de inicio de la auditoría a realizar.

Se realizará verificación de aplicación de los procedimientos evaluados en la sede central del GNTID.

Se evaluarán las unidades auditables que hacen parte del Subsistema de Seguridad de la Información, así: Gestión de incidentes de la Seguridad de la Información, Gestión de incidentes de Tecnologías de la Información, Gestión de la Capacidad de las Tecnologías de la Información y Gestión Del Cambio en La Infraestructura de Tecnologías de La Información.

CRITERIOS DE AUDITORIA:

CRITERIOS DE AUDITORIA:

NTC ISO/IEC 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

Manuales, Guías, Instructivos y demás documentos aplicados a 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, Lineamientos Generales de la Política de Gobierno Digital

Decreto No. 1078 de 2015 Libro 2, parte 2, título 9. Cap. 1.- I Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones.

y demás normatividad externa vigente. (Ley 1712 de 2014 - Ley de Transparencia y Acceso a la Información, entre otras)

AUDITOR LÍDER:	AUDITOR(ES) ACOMPAÑANTE(S)	EXPERTO(S) TÉCNICO(S)	AUDITOR (ES) EN FORMACIÓN
HENRY CORTÉS CONTRERAS	NO APLICA	ALEXANDRA ROA CAICEDO	NO APLICA



A continuación se presentan las no conformidades y un resumen de los aspectos favorables y evidencias de la Auditoría a dos unidades auditables (1) Proceso de Gestión de Infraestructura Tecnológica y Servicios Informáticos y (2) Sistema de Gestión de la Seguridad de la Información, así como la conclusión registrada en el informe original.

ASPECTOS FAVORABLES

1. Disposición de los responsables de los procesos en el suministro de la información.
2. Proactividad de los auditados durante la etapa de ejecución de la auditoría.

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

Descripción:	No se asegura que las personas sean competentes, basándose en la educación, formación o experiencias adecuadas para la implementación de los roles de que puedan afectar el desempeño del sistema de la seguridad de la información.
Requisito aplicable:	1. NORMA NTC/ISO 27001:2013: Numeral 7.2. b) - Competencia – personas que sean competentes, basándose en la educación, formación o experiencias adecuadas y 7.2 c) Conservar la información documentada apropiada, como evidencia de la competencia. 2. RESOLUCIÓN No.000837 de 2019 - Artículo 8: Roles y Responsabilidades de los intervinientes en la organización de la Seguridad de la Información. 3. MIPG - 7ª DIMENSIÓN – Componente Ambiente de Control.
Evidencia objetiva:	Los documentos suministrados por el equipo auditado no evidencian lo establecido en el numeral 7.2.c) de la Norma 27001:2013, solo describen la siguiente información: a. En el documento denominado “Análisis Roles-GNTIC-GND-PDF”, se encuentran descritos los roles y funciones de los cargos basados en la Resolución No.000015 de 2014, la cual no se encuentra vigente, siendo necesario definir para los roles de los integrantes de la implementación del SGSI (Artículo 8 de la Resolución No.000837 de 2019) la educación, formación o experiencia adecuada que establece la Norma 27001:2013 en el numeral 7.2.b). b. En el Oficio N°134-GNTIC-DG-2019, de fecha 10 de mayo, dirigido a la Dirección General, relacionan las actividades, funciones y cargos desempeñados por los servidores públicos que integran el GNTID, sin que dentro de este documento se definan los roles establecidos en Resolución No.000837 de 2019 y la educación, formación y experiencia adecuada requerida en el artículo 7.2 b) de la Norma 27001:2013. En el documento de “Referencia para las funciones del área de TI” (versión 1 del 21 de febrero de 2019), no se encuentran definidos los roles, formación educativa y experiencia adecuada expresadas en la Resolución No.000837 de 2019.

NO CONFORMIDAD No. 2

Descripción:	No se garantiza que la información documentada requerida por el Sistema de la Seguridad de la Información, esté disponible y adecuada para el uso, donde y cuando se necesita.
---------------------	--

**Requisito aplicable:**

- 1. NORMA 27001:2013** – Numeral 7.5.3 - Control de Información Documentada.
- 2. PROCEDIMIENTO DE CONTROL DE REGISTROS** – Código DG-E-P-002 - Actividad 7.4.1. - Identificar Los Registros Del Sistema Integrado De Gestión Por Controlar.
- 3. MIPG - 7ª Dimensión** – Componentes Actividades de Control.

Evidencia objetiva:

- a. No se dispone de un control de Registros para el control de Copias de Respaldo de los aplicativos o sistemas de información institucional.
- b. No se dispone de control de registros en el Aplicativo OTRS para control de trazabilidad sobre los soportes prestados a los aplicativos o sistemas de información Institucional (desde la solicitud del requerimiento o soporte hasta la respuesta o entrega de la solución).
- c. No se cuenta con un procedimiento actualizado para El diseño y desarrollo de Aplicativos o Sistemas de Información del Instituto donde se establezca los lineamientos y estándares que deben ser aplicados dentro del equipo de profesionales que desarrollan esta actividad en la entidad. Aunque se cuenta con un documento denominado “Guía de Gestión de Aplicaciones”, creado en su versión 1, el 14 de abril 2018, versión 1.1, para el 14 de mayo de 2020, no se encuentra incluido dentro del aplicativo ISOLUCION.
- d. La Resolución No.000837 de 2019, debe ser actualizada debido a que ella tiene las siguientes inconsistencias:
 - Se registra el perfil de “Facilitadores Regionales de Tecnologías de Información y Comunicaciones”, siendo el nombre correcto Facilitadores Regionales de Tecnologías de Información y Desarrollo.
 - Dentro de las funciones que los facilitadores Regionales se encuentra: “Rendir informes a los Directores Regionales”, pero en algunas regionales los facilitadores dependen del Grupo Regional Administrativo y Financiero como Noroccidente y Oriente.
 - El alcance registrado en la Resolución no está alineado con el alcance que aparece en el Manual del SIG.

NO CONFORMIDAD No. 3**Descripción:**

No se garantiza la comunicación interna y externa pertinente que contribuya al Sistema Integrado de Gestión y a la implementación del Sistema de Gestión de la Seguridad de la Información.



INSTITUTO NACIONAL DE MEDICINA LEGAL Y CIENCIAS FORENSES

INFORME EJECUTIVO DE AUDITORÍA

Página 4 de 6

Requisito aplicable:

- 1. NORMA 27001:2013** – Numeral 7.4 Comunicación.
- 2. Procedimiento de Evaluación de Satisfacción al cliente** – DG-C-P002-V10. Actividad 3.3: Difundir entre el personal a cargo, los resultados de la Evaluación de Satisfacción del Cliente.
- 3. MIPG - 7ª Dimensión** – Componentes Actividades de Control y Información y Comunicación.

Evidencia objetiva:

No se aportaron evidencias de la difusión de los resultados de la Evaluación de la Satisfacción al Cliente vigencia 2019, Al interior del Grupo Nacional de Tecnologías de la Información y hacia los Facilitadores Regionales de Tecnologías de la Información.

NO CONFORMIDAD No. 4

Descripción:

No se han identificado, analizado y valorado los riesgos de seguridad digital y aquellos que afecten el SGSI.

Requisito aplicable:

- 1. NORMA 27001:2013** – Numerales 8.2 y 8.3.
- 2. Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas.** Riesgos de Gestión, De Corrupción y de Seguridad Digital. Versión 4 – Año 2018. Departamento Administrativo de la Función Pública.
- 3. Resolución No.000858 de 2019 (4 de diciembre)** - Política de Gestión del Riesgo del INMLYCF. Artículo 8 – Tipificación de los Riesgos Instituciones.
- 4. MIPG - 7ª Dimensión** – Componente de Evaluación del Riesgo

Evidencia objetiva:

- En el Informe de Seguimiento de Riesgos Institucionales del Primer y Segundo Cuatrimestre de 2020, elaborado por la Oficina de Control Interno, se reitera la incorporación de los riesgos de seguridad digital.
- Aunque se cuenta con una primera prueba en la identificación de riesgos de seguridad digital, aún no se cuenta con un registro de los mencionados riesgos dentro del mapa de riesgos institucional.



OPORTUNIDADES DE MEJORA

1. Garantizar la actualización de la caracterización y los documentos asociados al Proceso de Gestión de la Infraestructura Tecnológica y Servicios Informáticos, teniendo en cuenta las recomendaciones dadas durante el proceso de la auditoría, en cuanto al objetivo definido, los documentos asociados, la normatividad aplicada, entre otros.
2. Los indicadores vigentes del Proceso de Gestión de la Infraestructura Tecnológica y Servicios Informáticos requieren alinearse con la caracterización, de tal forma que garanticen el desempeño de los servicios generados. Entre los indicadores a incluir deben estar: (a) la medición de la capacidad Tecnológica del Instituto; (b) la medición de la Gestión relacionada con el Soporte a las aplicaciones o sistemas de información; (c) los tres indicadores que midan los objetivos incluidos dentro de la Resolución No.000837 de 2019. Por otro lado, se debe excluir el indicador de satisfacción de usuarios Externos.
3. Alinear los documentos para que garanticen que la estructura organizacional sea la misma a nivel nacional, ya que en algunas regionales el facilitador aparece dependiente del Grupo Regional Administrativo y Financiero (Caso Regionales Oriente y Noroccidente), lo cual no es coherente con las funciones establecidas en la Resolución No.00837 de 2019, Artículo 8, Numeral 5 - e) Funciones de los Facilitadores Regionales de Tecnologías de la Información y Comunicaciones.
4. Se realicen las gestiones ante la Dirección General para la asignar la función de líder de Seguridad de la Información, acorde a lo establecido en el artículo 10, Designación del Líder de Seguridad de la Información de la Resolución No.000837 de 2019.
5. Incluir dentro de las No Conformidades NCP 743, NCP 750, acciones que ayuden a mitigar las causas tales como: evaluar la comprensión de la sensibilización y toma de conciencia en el Sistema de Gestión de la Seguridad de la Información, verificar los resultados en el aplicativo de OTRS, relacionados con aspectos de la seguridad de la información (incidentes de seguridad, protección de los activos de la información y aplicación de políticas y controles a servidores públicos, contratistas y terceros).
6. Fortalecer espacios de participación entre los integrantes del GNTID y los facilitadores Regionales de Tecnologías de la Información para la apropiación del conocimiento y aplicación de los documentos del SIG que le son atinentes a los procesos asociados al SGSI y al Proceso de Gestión de la Infraestructura Tecnológica y Servicios Informáticos.
7. Diseñar un plan de trabajo que incluya: las actividades, responsables, tiempos, productos o servicios generados, nivel de avance, entre otros, de tal forma que se garantice un seguimiento oportuno a las acciones pertinentes al GNTID, y por ende, se tomen los correctivos necesarios a fin de cumplir los objetivos previstos.
8. Que la actualización del listado maestro de registros se realice con mayor frecuencia debido a los cambios de los documentos del SIG
9. Acondicionar técnicamente el cuarto donde se encuentra el Puerto de Rack y UPS de la sede de la Regional Oriente, colocando medidor de temperatura, mientras son trasladados a la sede de la Regional Oriente que está siendo construida en el Municipio de Soacha.
10. Acorde al informe de vulnerabilidades de 2020 presentado por el GNTID, se hace necesario actualizar las causas y efectos del riesgo que aparece registrado en el Mapa de Riesgos Institucional denominado "*Posibles Vulnerabilidades sobre los Sistemas de Información y Plataformas Tecnológicas*", teniendo en cuenta las causas tales como: versión de apache expuesta a múltiples ataques, servidor PHP expuesto a múltiples vulnerabilidades, en criticidad media/alta, protocolos susceptibles a identificación de credenciales, información sensible viajando en texto plano y política de password insegura. Las mencionadas causas se



encuentran dentro del informe mencionado y requiere para cada una de ellas establecer las acciones correspondientes.

CONCLUSIONES DE LA AUDITORÍA

Al realizar la verificaron las actividades desarrolladas para el Proceso de Gestión de Infraestructura Tecnológica y Servicios Informáticos y el Sistema de Gestión de la Seguridad de la Información, y según los resultados obtenidos en el presente informe, se puede concluir que se viene cumpliendo con la normatividad vigente y los documentos contemplados en el SIG, respecto a las dos unidades auditables, no obstante; existen algunas debilidades tales como la incorporación de: (a) los riesgos de seguridad digital en el Mapa de riesgos Institucional, (b) Seguimiento periódico a los controles de los riesgos institucionales acorde a la frecuencia y el responsable de su verificación (b) la inclusión de los indicadores que miden los objetivos de la Política del SGSI, (c) La incorporación de acciones en algunas No Conformidades de los procesos evaluados y (d) la actualización oportuna de los documentos asociados a la caracterización, de tal manera que contribuyan a la eficacia de los servicios prestados por las unidades auditables.

Con ocasión de la emergencia sanitaria COVID-19 en todo territorio nacional, esta auditoría aplicó el documento internacional IAF-MD4:2018, incluido protocolo de los roles para la realización de auditorías remotas en el INMLYCF tal como lo establece el Memorando No. 052-DG-2020 (21 de mayo).

Se realizó parte de la etapa de ejecución en forma remota y otra en forma 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 denominada Jitsi Meeting, autorizada por Instituto; la comunicación fue óptima y los dispositivos utilizados no tuvieron ningún contratiempo.

AUTOR LÍDER DEL INFORME (Nombre y firma)**FECHA DE ELABORACIÓN****HENRY CORTES CONTRERAS****2020-12-04**