INSTITUTO NACIONAL DE SALUD

INFORME DE SEGURIDAD DE LA INFORMACION
BOGOTA, 2022

Av. Calle 26 No. 51- 20, Bogotá, D.C., Colombia
Conmutador: (1) 220 7700 Ext. 1703-1704
correo electrónico: contactenos@ins.gov.co
Página web: **www.ins.gov.co**
Línea gratuita nacional: 018000 113 400

AVISO DE CONFIDENCIALIDAD

La información confidencial, y todos los derechos a la misma que han sido o serán divulgados en este documento, permanecerán como propiedad del INSTITUTO NACIONAL DE SALUD. Este documento bajo la condición de confidencialidad mutua, donde las partes deben respetar la información provista. Por lo tanto, la información contenidaen este documento y en los medios magnéticos entregados es de carácter reservadoy sólo puede ser utilizado por el personal que el INSTITUTO NACIONAL DE SALUD, designe para su revisión, resguardo, manipulación y/o divulgación. Las normas que fundamentan el carácter reservado de la información.

CONTROL DE DOCUMENTOS

VERSIÓN	FECHA DE APROBACIÓN			DESCRIPCIÓN
	aaaa	mm	dd	
0	2022	07	08	Creación del documento

	ELABORO	REVISO	APROBO
INSTITUTO NACIONAL DE SALUD MINISTERIO DE SALUD Y PROTECCIÓN SOCIAL	Ricardo casimilas	Roger Smith Londoño	Elsa Marlen Baracaldo Huertas
	Profesional	Profesional Especializado	Jefe de TI

Av. Calle 26 No. 51- 20, Bogotá, D.C., Colombia
Conmutador: (1) 220 7700 Ext. 1703-1704
correo electrónico: contactenos@ins.gov.co
Página web: **www.ins.gov.co**
Línea gratuita nacional: 018000 113 400

TABLA DE CONTENIDO

Tabla de contenido

Av. Calle 26 No. 51- 20, Bogotá, D.C., Colombia
Conmutador: (1) 220 7700 Ext. 1703-1704
correo electrónico: contactenos@ins.gov.co
Página web: **www.ins.gov.co**
Línea gratuita nacional: 018000 113 400

INTRODUCCIÓN

El presente informe incluye el respectivo análisis de las amenazas,vulnerabilidades y los resultados de la identificación, valoración y tratamiento delos riesgos de seguridad de la información, a saber: procesos de soporte (gestión humana; gestión de seguridad y gestión de tecnologías de la información), realizado con base en el *"Instructivo para el proceso de inventario, clasificación activos de información",* y la *"Metodología de análisis, evaluación y tratamiento de riesgos".*

Así mismo se puede evidenciar la identificación de controles necesarios para mitigar o transferir los riesgos identificados para los procesos del alcance del SGSI del Instituto Nacional de salud, como resultado de la aplicación de lametodología definida.

1. METODOLOGÍA DESARROLLADA

La identificación de las amenazas y de las vulnerabilidades, análisis de impacto e identificación de controles para mitigar los riesgos de Seguridad de la Información, se realizaron por medio de entrevistas donde, inicialmente, se identificaron los activos de información tipificados como: personas, software, infraestructura, información, hardware, servicios y bases de datos, en los procesos establecidos en el alcance del proyecto Sistema de Gestión de Seguridad de la Información (SGSI), a saber, complementado con la metodología descrita en el "Instructivo para el proceso de inventario, clasificación activos de información", así mismo se realizó la identificación de los riesgos, amenazas, vulnerabilidades asociadas a los activos de información, para posterior realizar la identificación y la evaluación los controles implementados en la Entidad para la gestión de los riesgos de acuerdo a la "Metodología de análisis, evaluación y tratamiento de riesgos".

- Documentación: El análisis de la documentación existente en el INS es el soporte y la evidencia para verificar el nivel de implementación de cada cláusula y de cada objetivo de control del estándar.

- Instrumento de Evaluación: Elaboración del instrumento para el Análisis de Brechas.

- Nivel de Madurez: Definir la escala de madurez para la evaluación del estado actual.

- Entrevistas: En las entrevistas se determina con cada área según el dominio a ser analizado, el estado de cumplimiento de cada una de las cláusulas y objetivos de control del estándar y su nivel de madurez.

- Análisis de Brechas: Revisión del cumplimiento y el nivel de madurez para cada uno de los requerimientos Mandatorios y del Anexo A, el cual se realizará como se describe a continuación:
    - Identificar y registrar las evidencias de implementación de cada requisito del estándar.

Av. Calle 26 No. 51- 20, Bogotá, D.C., Colombia
Conmutador: (1) 220 7700 Ext. 1703-1704
correo electrónico: contactenos@ins.gov.co
Página web: www.ins.gov.co
Línea gratuita nacional: 018000 113 400

- Asignar una valoración cualitativa de cada requerimiento, según las evidencias identificadas de acuerdo a la valoración de la Tabla 4. Escala de valoración del cumplimiento.

➢ Definir el nivel de Madurez Actual frente a las buenas prácticas establecidas en la norma para el cumplimiento de la ISO/IEC 27001, como se puede apreciar en la Tabla 4. Escala de nivel de Madurez del SGSI.

Áreas entrevistadas.

Entrevista	Tiempo
R01 - Redes en Salud Pública	2 horas
R02 - Vigilancia y Análisis del Riesgo en Salud Pública	2 horas
R03 - Investigación en Salud Pública	2 horas
R04 - Producción	2 horas
R05 - Observatorio Nacional de Salud	2 horas
A01 - Gestión Humana	2 horas
A02 - Adquisición de Bienes y Servicios	2 horas
A03 - Gestión Documental	2 horas
A04 - Equipos de Laboratorio	2 horas
A05 - Gestión Ambiental	2 horas
A07 - Gestión Jurídica	2 horas
A08 - Atención al Ciudadano	2 horas
A09 - Gestión Financiera	2 horas
A10 - Recursos Físicos	2 horas
D01 - Planeación Institucional	2 horas
D02 - Gestión de Calidad	2 horas
D03 - Comunicación Institucional	2 horas
D04 - Tecnologías de Información y Comunicaciones	2 horas
E01 - Control Interno Institucional	2 horas
Dirección General - Asesores	2 horas
Dirección General	2 horas
Secretaría General	2 horas
Secretaria General - Asesores	2 horas

2. ANÁLISIS DE AMENAZAS

De acuerdo con lo planteado y definido en la norma ISO/IEC 27005 “Las amenazas pueden ser deliberadas, accidentales o ambientales (naturales) y pueden dar como resultado, por ejemplo, daños o pérdidas de serviciosesenciales” por lo anterior es relevante la evaluación de las amenazas las cuales podrían explotar vulnerabilidades, afectando de manera significativa la confidencialidad, integridad y disponibilidad de la información para el Instituto Nacional de Salud

Para la identificación de amenazas de Seguridad de la Información, se utilizó el siguiente inventario:

Av. Calle 26 No. 51- 20, Bogotá, D.C., Colombia
Conmutador: (1) 220 7700 Ext. 1703-1704
correo electrónico: contactenos@ins.gov.co
Página web: www.ins.gov.co
Línea gratuita nacional: 018000 113 400

2.1 Inventario de Amenazas de Seguridad de la Información

INCUMPLIMIENTO EN EL MANTENIMIENTO DEL SISTEMA DE INFORMACIÓN.	INCUMPLIMIENTO EN EL MANTENIMIENTO DEL SISTEMA DE INFORMACIÓN.
DESTRUCCIÓN DE EQUIPOS O DE MEDIOS.	DESTRUCCIÓN DE EQUIPOS O DE MEDIOS.
POLVO, CORROSIÓN, CONGELAMIENTO.	POLVO, CORROSIÓN, CONGELAMIENTO.
ERROR EN EL USO	ERROR EN EL USO
PÉRDIDA DEL SUMINISTRO DE ENERGÍA.	PÉRDIDA DEL SUMINISTRO DE ENERGÍA.
FENÓMENOS METEOROLÓGICOS.	FENÓMENOS METEOROLÓGICOS.
HURTO DE MEDIOS O DOCUMENTOS.	HURTO DE MEDIOS O DOCUMENTOS.
ABUSO DE DERECHOS.	ABUSO DE DERECHOS.
CORRUPCIÓN DE DATOS.	CORRUPCIÓN DE DATOS.
ERROR EN EL USO.	ERROR EN EL USO.
FALSIFICACIÓN DE DERECHOS.	FALSIFICACIÓN DE DERECHOS.
PROCESAMIENTO ILEGAL DE DATOS.	PROCESAMIENTO ILEGAL DE DATOS.
MAL FUNCIONAMIENTO DEL SOFTWARE	MAL FUNCIONAMIENTO DEL SOFTWARE
MAL FUNCIONAMIENTO DEL SOFTWARE.	MAL FUNCIONAMIENTO DEL SOFTWARE.
MANIPULACIÓN DE SOFTWARE.	MANIPULACIÓN DE SOFTWARE.
USO NO AUTORIZADO DEL EQUIPO O SOFTWARE.	USO NO AUTORIZADO DEL EQUIPO O SOFTWARE.
NEGACIÓN DE ACCIONES.	NEGACIÓN DE ACCIONES.
ESCUCHA ENCUBIERTA.	ESCUCHA ENCUBIERTA.
FALLA DE EQUIPO DE TELECOMUNICACIONES.	FALLA DE EQUIPO DE TELECOMUNICACIONES.
ESPIONAJE REMOTO.	ESPIONAJE REMOTO.
SATURACIÓN DEL SISTEMA DE INFORMACIÓN.	SATURACIÓN DEL SISTEMA DE INFORMACIÓN.
INCUMPLIMIENTO EN LA DISPONIBILIDAD DEL PERSONAL	INCUMPLIMIENTO EN LA DISPONIBILIDAD DEL PERSONAL
DESTRUCCIÓN DE EQUIPOS O MEDIOS	DESTRUCCIÓN DE EQUIPOS O MEDIOS
PROCESAMIENTO ILEGAL DE LOS DATOS.	PROCESAMIENTO ILEGAL DE LOS DATOS.
DATOS PROVENIENTES DE FUENTES NO CONFIABLES.	DATOS PROVENIENTES DE FUENTES NO CONFIABLES.
FALLA DEL EQUIPO.	FALLA DEL EQUIPO.

Av. Calle 26 No. 51- 20, Bogotá, D.C., Colombia
Conmutador: (1) 220 7700 Ext. 1703-1704
correo electrónico: contactenos@ins.gov.co
Página web: **www.ins.gov.co**
Línea gratuita nacional: 018000 113 400

2.2. Amenazas por proceso

Según el análisis realizado a los procesos del alcance, se pudo identificar lassiguientes amenazas:

Amenazas comunes de los procesos extremo

AMENAZAS DENTIFICADAS	EXTREMO
Actividad de Vandalismo	N/A
Actividad Maliciosa de Ciberdelincuente	1
corrupción de datos	3
Divulgación	1
Falla del Equipo	4
Fenómenos sísmicos	1
Fuego	2
Hurto de equipo	6
Hurto de medios o documentos	1
Mal funcionamiento del software	N/A
Procesamiento ilegal de datos	N/A
Uso no autorizado del equipo	1
TOTAL EN %	31,9%

Amenazas comunes de los procesos altos.

AMENAZAS DENTIFICADAS	ALTO
Actividad de Vandalismo	1
Actividad Maliciosa de Ciberdelincuente	N/A
corrupción de datos	3
Divulgación	N/A
Falla del Equipo	N/A
Fenómenos sísmicos	1
Fuego	N/A
Hurto de equipo	2
Hurto de medios o documentos	N/A
Mal funcionamiento del software	N/A
Procesamiento ilegal de datos	1
Uso no autorizado del equipo	2
TOTAL EN %	13,5%

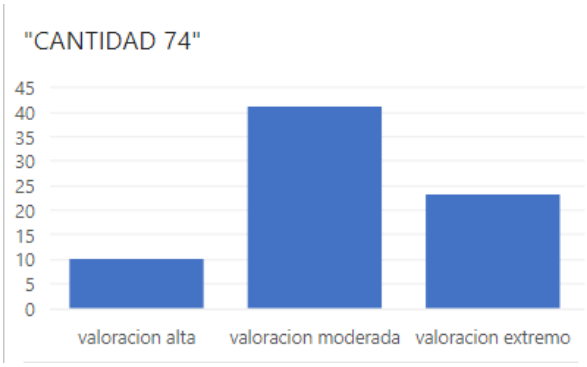
Av. Calle 26 No. 51- 20, Bogotá, D.C., Colombia
Conmutador: (1) 220 7700 Ext. 1703-1704
correo electrónico: contactenos@ins.gov.co
Página web: **www.ins.gov.co**
Línea gratuita nacional: 018000 113 400

Amenazas comunes de los procesos moderados

AMENAZAS DENTIFICADAS	MODERADO
Actividad de Vandalismo	N/A
Actividad Maliciosa de Ciberdelincuente	N/A
corrupción de datos	3
Divulgación	N/A
Falla del Equipo	N/A
Fenómenos sísmicos	N/A
Fuego	5
Hurto de equipo	N/A
Hurto de medios o documentos	12
Mal funcionamiento del software	1
Procesamiento ilegal de datos	3
Uso no autorizado del equipo	18
TOTAL EN %	55,40%

2.3 Análisis de los Resultados

De manera general se puede identificar que la evaluación del riesgo con mayor cantidad para la Seguridad de la Información entre los resultados obtenidos de los procesos analizados, se relaciona como nos muestra el grafico



Del total de riesgos identificados, las cuales se asocian a vulnerabilidades como el mantenimiento no adecuado de equipos o hardware; errores humanos, falta de actualizaciones, entre otras, que pueden ser explotadas materializando riesgos como fallas o pérdida del servicio, daño o mal funcionamiento de los sistemas de información y equipos tecnológicos.

Por otro lado se identifica la valoración extrema la amenaza Hurto de equipo con una recurrencia de 6 veces, en la evaluación moderada la amenaza Uso no autorizado del equipo tiene una recurrencia de 18 veces y en la evaluación alta la amenaza s, Hurto de equipo y Uso no autorizado replica con 2 veces cada una teniendo en cuenta que los sistemas de información y las telecomunicaciones de la entidad son un aspecto relevante para mantener la oportuna operación de la entidad, se puede evidenciar para estos tipos de amenazas las relacionadas con el aprovisionamiento o cobertura insuficiente en el

Av. Calle 26 No. 51- 20, Bogotá, D.C., Colombia
Conmutador: (1) 220 7700 Ext. 1703-1704
correo electrónico: contactenos@ins.gov.co
Página web: www.ins.gov.co
Línea gratuita nacional: 018000 113 400

control, llevando un formato para el manejo adecuado de entrega y devoluciones de equipos.

3. ANALISIS DE VULNERABILIDADES

Para el estándar ISO/IEC 27005:2011, las vulnerabilidades son debilidades internas "que son explotadas por amenazas con el objetivo de poner en peligro los activos principales (procesos e información)", por tanto, contrario a las amenazas son factores y variables que si son controladas por la Entidad, la cual puede definir acciones que requieren realizar evaluaciones periódicas de los controles definidos por el Instituto Nacional de Salud, con el fin de que estos sean efectivos evitando así la aparición de brechas e incluso de nuevas vulnerabilidades.

Por lo anterior resulta relevante definir controles para la mitigación de las vulnerabilidades técnicas que a su vez pueden ser explotadas por una amenaza, como por ejemplo, el hacking no ético y materializar riesgos como intrusiones, accesos no autorizados, modificación de información o configuración, que puedan afectar tanto la seguridad de la información como la continuidad del negocio de la Entidad.

3.1 Identificación de vulnerabilidades

Según las Amenazas con mayor porcentaje de impacto para la Seguridad de la Información de la INS, se relacionan las vulnerabilidades con probabilidad de materialización.

Fallas Generales / Daños					
Aprovisionamiento o cobertura insuficiente de los servicios	Error Humano	Ausencia de Soporte por parte del Fabricante	Administración de Dispositivos de Red Insuficiente	Falta de mantenimiento y actualización de los sistemas de información	Mantenimiento no adecuado de equipos y HW
Casos fortuitos (Inundación, incendio, entre otras)					
Infraestructura de almacenamiento no adecuada.	Ausencia de unsistema de continuidad de negocio	Ausencia de un refuerzo estructural de las instalaciones	Ubicación físicade los equipos	Infraestructura de almacenamiento no adecuada.	Ausencia de un sistema de continuidad de negocio
Errores de Software					

Av. Calle 26 No. 51- 20, Bogotá, D.C., Colombia
Conmutador: (1) 220 7700 Ext. 1703-1704
correo electrónico: contactenos@ins.gov.co
Página web: www.ins.gov.co
Línea gratuita nacional: 018000 113 400

Ausencia de una configuración segura del aplicativo	Error Humano	Falla en el sistema de información	Ausencia de Soporte por parte del Fabricante	Definición no adecuada de los acuerdos con los proveedores	Ausencia de una configuración segura del aplicativo

Virus Informático					
Ausencia de (antivirus)	**Ausencia de copias de respaldo**	**Ausencia de un respaldo de las Bases de Datos**	**Espacio insuficiente en los servidores de la Entidad**	**Ausencia de actualización y mantenimiento del software**	Error Humano

Fallo de servicios de comunicaciones				
Fallas del servidor de la Entidad	Ausencia de un sistema de continuidad de negocio	Ausencia de servicio disponible por dependencia de terceros	Ausencia de contingencia de prestador de servicio de líneas para la conexión con la Planta telefónica	Definición no adecuada de los acuerdos con los proveedores

3.2 Análisis de los Resultados

Se identificó que entre las vulnerabilidades más representativas que pudieranllegar a afectar a la Entidad se encuentran:

- Ausencia de un proceso de continuidad del negocio, Ausencia de Soporte por parte del Fabricante, Definición no adecuada de los acuerdos con los proveedores, Aprovisionamiento o cobertura insuficiente de los servicios: Dichas vulnerabilidades se asocian debido a que afectan de manera significativa la integridad y disponibilidad delos activos de información que requieren soporte o mantenimiento por parte de un proveedor y/o alta disponibilidad como recuperación inmediata, por tanto se recomienda como parte del tratamiento de riesgos, definir ANS de los servicios más críticos prestados por terceros, así como, la ejecución de planes de continuidad documentados y que sean de conocimiento de las áreas interesadas con el fin de hacer seguimiento al cumplimiento de los mismos evitando el daño o mal funcionamiento de sistemas de información y demás activos de información que requieren intervención de terceros para su adecuado funcionamiento.

Av. Calle 26 No. 51- 20, Bogotá, D.C., Colombia
Conmutador: (1) 220 7700 Ext. 1703-1704
correo electrónico: contactenos@ins.gov.co
Página web: www.ins.gov.co
Línea gratuita nacional: 018000 113 400

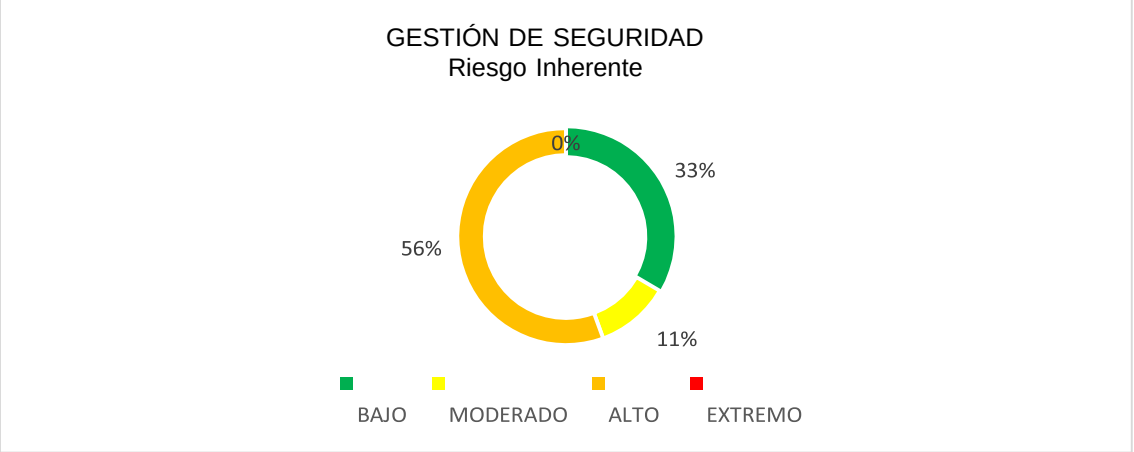
- Error humano: Esta vulnerabilidad está asociada a la posible materialización de riesgos tales como diligenciamiento errado o incompleto, modificación sin autorización, daño o perdida de información en formato físico o digital, para lo cual es importante definir planes de tratamiento focalizados en la capacitación y re-inducción de los funcionarios nuevos y existentes de la Entidad, así como la estructuración de procedimientos que permitan validar la integridad de la información ingresada, salvaguardando la integridad de la información.

Los riesgos que se podrían materializar ante las vulnerabilidades identificadas hacen referencia a la pérdida de información en formato digital, denegación del servicio, daño o mal funcionamiento de los sistemas de información, para lo cual es necesario que la INS, cuente con programas de mantenimiento de los sistemas de información y de la infraestructura tecnológica, donde se asegure los mantenimientos preventivos y planes de acción pertinentes que garanticen el funcionamiento adecuado de los activos de información relacionados con el software, hardware e instalaciones.

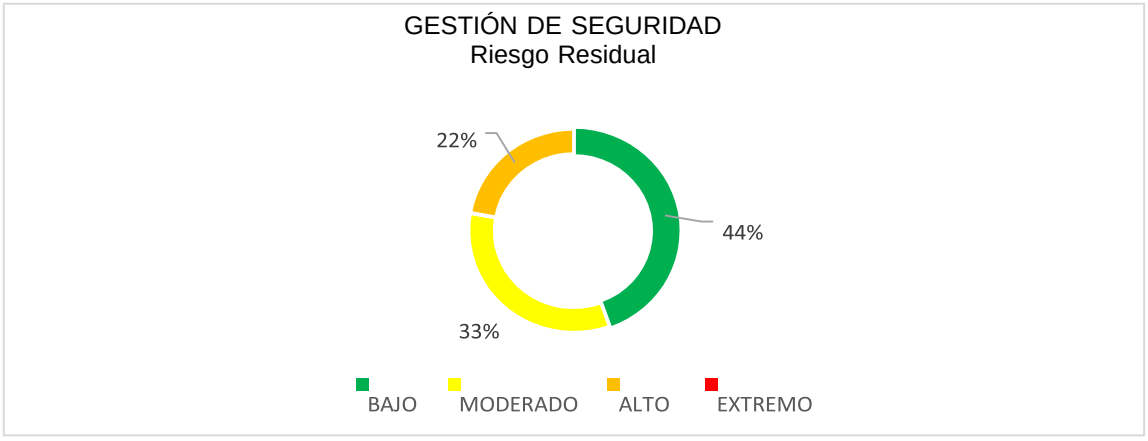
4. IDENTIFICACIÓN, VALORACIÓN Y TRATAMIENTO DE RIESGOS

Para la evaluación de riesgos se tuvieron en cuenta las amenazas y vulnerabilidades anteriormente relacionadas que afectan la Seguridad de la Información de la Entidad, por lo tanto los resultados obtenidos están orientados ala mitigación de los riesgos provocados por la explotación de dichas amenazas y vulnerabilidades. La respectiva identificación y valoración se realizó con la “Metodología de análisis, evaluación y tratamiento de riesgos**”.**

4.1 Análisis general para la mitigación de los riesgos en Gestión de Seguridad de la información.



Av. Calle 26 No. 51- 20, Bogotá, D.C., Colombia
Conmutador: (1) 220 7700 Ext. 1703-1704
correo electrónico: contactenos@ins.gov.co
Página web: **www.ins.gov.co**
Línea gratuita nacional: 018000 113 400



Para el proceso objeto del análisis se puede evidenciar un desplazamiento importante de los riesgos inherentes, ubicándose residualmente el 77%(33%+44%) en la zona aceptable, para el 22% de los riesgos asociados a la zona alta, es importante reducir, evitar, compartir o transferir el riesgo.

Promedio general del sistema de gestión de seguridad de la Información (SGSI)

Av. Calle 26 No. 51- 20, Bogotá, D.C., Colombia
Conmutador: (1) 220 7700 Ext. 1703-1704
correo electrónico: contactenos@ins.gov.co
Página web: **www.ins.gov.co**
Línea gratuita nacional: 018000 113 400

Nivel de los controles del Anexo A de la ISO 27001

4.2 Recomendaciones

- Es transcendental definir las acciones, los responsables y la fecha de ejecuciónde los planes de tratamiento de riesgos que se encuentran fuera del apetito de riesgo, así mismo se requiere hacer un seguimiento periódico para evaluar el

  avance de las actividades definidas con el fin de dar cumplimiento a los planes sugeridos y así gestionar y disminuir el nivel de los riesgos extremos y altos, propendiendo por el mejoramiento continuo del Sistema de Gestión de Seguridad de la Información.

- Para la culminación de los controles asociados, es importante que se revalúe y obtenga el nuevo nivel de riesgo. Adicionalmente se sugiere realizar una auditoría de sistemas de información que permita evaluar los aspectos relacionados con control interno relacionados con los activos de información y los riesgos asociados.

Av. Calle 26 No. 51- 20, Bogotá, D.C., Colombia
Conmutador: (1) 220 7700 Ext. 1703-1704
correo electrónico: contactenos@ins.gov.co
Página web: **www.ins.gov.co**
Línea gratuita nacional: 018000 113 400

NORMATIVIDAD APLICABLE

- Norma Técnica Colombiana NTC-ISO-IEC 27001:2013, Tecnología de la Información, Técnicas de Seguridad, Sistemas de Gestión de la Seguridad de la Información, Requisitos, 2013-12-11, ICONTEC Internacional.

- Norma Técnica Colombiana NTC-ISO-IEC 27002:2013, Guía de Implementación Sistemas de Gestión de la Seguridad de la Información, 2013- 12-11, ICONTEC Internacional.

- Norma Técnica ISO-IEC 27005:2011, Tecnología de la Información, Técnicas de Seguridad, Administración de Riesgos de Seguridad de la Información, 2011-06-01, ISO.

REFERENCIAS

- ISO-IEC 27001:2013, 2013-12-11, ICONTEC Internacional, http://www.icontec.org/Paginas/e_normas.aspx

- Norma Técnica ISO-IEC 27005:2013, 2011-06-01, ISO, https://www.iso.org/standard/56742.html

- Ministerio de Tecnologías de la Información y las Comunicaciones, Guía No. 5 de Gobierno en Línea "Guía para la Gestión y Clasificación de Activos de Información", http://www.mintic.gov.co/gestionti/615/articles-5482_G5_Gestion_Clasificacion.pdf

- Ministerio de Tecnologías de la Información y las Comunicaciones, Guía N°7 "Guía de Gestión de Riesgos", http://www.mintic.gov.co/gestionti/615/articles-5482_G7_Gestion_Riesgos.pdf

- Matriz de Riesgos del SGSI

  https://inssalud.sharepoint.com/:x:/r/sites/SGSI/_layouts/15/Doc.aspx?sourcedoc=%7BB6B08575-7E06-4D60-96B3-8C774858A875%7D&file=FOR-D04.0000-011.xlsx&action=default&mobileredirect=true

- Departamento Administrativo de la Función Pública (DAFP), Guía para la Administración del Riesgo, https://www.funcionpublica.gov.co/documents/418537/506911/1592.pdf/73e5a159-2d8f-41aa-8182-eb99e8c4f3ba