INSTITUTO NACIONAL DE SALUD

PLAN DE TRATAMIENTO Y RIESGOS SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

2018

Av. Calle 26 No. 51- 20, Bogotá, D.C., Colombia
Conmutador: (1) 220 7700 Ext. 1703-1704
fax: 220 7700 Ext. 1283-1269
correo electrónico: contactenos@ins.gov.co
Página web: **www.ins.gov.co**
Línea gratuita nacional: 018000 113 400

DEFINICIONES

Acceso a la Información Pública
Derecho fundamental consistente en la facultad que tienen todas las personas de conocer sobre la existencia y acceder a la información pública en posesión o bajo control de sujetos obligados. (Ley 1712 de 2014, art 4).

Activo
En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de la misma (sistemas, soportes, edificios, personas…) que tenga valor para la organización. (ISO/IEC 27000).

Activo de Información
En relación con la privacidad de la información, se refiere al activo que contiene información pública que el sujeto obligado genere, obtenga, adquiera, transforme o controlar en su calidad de tal.

Archivo
Conjunto de documentos, sea cual fuere su fecha, forma y soporte material, acumulados en un proceso natural por una persona o entidad pública o privada, en el transcurso de su gestión, conservados respetando aquel orden para servir como testimonio e información a la persona o institución que los produce y a los ciudadanos, o como fuentes de la historia. También se puede entender como la institución que está al servicio de la gestión administrativa, la información, la investigación y la cultura. (Ley 594 de 2000, art 3).

Amenazas
Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización. (ISO/IEC 27000).

Análisis de Riesgo
Proceso para comprender la naturaleza del riesgo y determinar el nivel de riesgo. (ISO/IEC 27000).

Auditoría
Proceso sistemático, independiente y documentado para obtener evidencias de auditoria y obviamente para determinar el grado en el que se cumplen los criterios de auditoria. (ISO/IEC 27000).

Autorización
Consentimiento previo, expreso e informado del Titular para llevar a cabo el Tratamiento de datos personales (Ley 1581 de 2012, art 3).

Bases de Datos Personales
Conjunto organizado de datos personales que sea objeto de Tratamiento (Ley 1581 de 2012, art 3).

Ciberseguridad

Capacidad del Estado para minimizar el nivel de riesgo al que están expuestos los ciudadanos, ante amenazas o incidentes de naturaleza cibernética. (CONPES 3701).

Ciberespacio

Es el ambiente tanto físico como virtual compuesto por computadores, sistemas computacionales, programas computacionales (software), redes de telecomunicaciones, datos e información que es utilizado para la interacción entre usuarios. (Resolución CRC 2258 de 2009).

Control

Las políticas, los procedimientos, las prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido. Control es también utilizado como sinónimo de salvaguarda o contramedida. En una definición más simple, es una medida que modifica el riesgo.

Datos Abiertos

Son todos aquellos datos primarios o sin procesar, que se encuentran en formatos estándar e interoperables que facilitan su acceso y reutilización, los cuales están bajo la custodia de las entidades públicas o privadas que cumplen con funciones públicas y que son puestos a disposición de cualquier ciudadano, de forma libre y sin restricciones, con el fin de que terceros puedan reutilizarlos y crear servicios derivados de los mismos (Ley 1712 de 2014, art 6).

Datos Personales

Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables. (Ley 1581 de 2012, art 3).

Datos Personales Públicos

Es el dato que no sea semiprivado, privado o sensible. Son considerados datos públicos, entre otros, los datos relativos al estado civil de las personas, a su profesión u oficio y a su calidad de comerciante o de servidor público. Por su naturaleza, los datos públicos pueden estar contenidos, entre otros, en registros públicos, documentos públicos, gacetas y boletines oficiales y sentencias judiciales debidamente ejecutoriadas que no estén sometidas a reserva. (Decreto 1377 de 2013, art 3).

Datos Personales Privados

Es el dato que por su naturaleza íntima o reservada sólo es relevante para el titular. (Ley 1581 de 2012, art 3 literal h).

Datos Personales Mixtos

Para efectos de esta guía es la información que contiene datos personales públicos junto con datos privados o sensibles.

Datos Personales Sensibles

Se entiende por datos sensibles aquellos que afectan la intimidad del Titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición, así como los datos relativos a la salud, a la vida sexual, y los datos biométricos. (Decreto 1377 de 2013, art 3).

Declaración de aplicabilidad

Documento que enumera los controles aplicados por el Sistema de Gestión de Seguridad de la Información – SGSI, de la organización tras el resultado de los procesos de evaluación y tratamiento de riesgos y su justificación, así como la justificación de las exclusiones de controles del anexo A de ISO 27001. (ISO/IEC 27000).

Derecho a la Intimidad

Derecho fundamental cuyo núcleo esencial lo constituye la existencia y goce de una órbita reservada en cada persona, exenta de la intervención del poder del Estado o de las intromisiones arbitrarias de la sociedad, que le permite a dicho individuo el pleno desarrollo de su vida personal, espiritual y cultural (Jurisprudencia Corte Constitucional).

Encargado del Tratamiento de Datos

Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, realice el Tratamiento de datos personales por cuenta del Responsable del Tratamiento. (Ley 1581 de 2012, art 3)

Gestión de incidentes de seguridad de la información

Procesos para detectar, reportar, evaluar, responder, tratar y aprender de los incidentes de seguridad de la información. (ISO/IEC 27000).

Información Pública Clasificada

Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, pertenece al ámbito propio, particular y privado o semiprivado de una persona natural o jurídica por lo que su acceso podrá ser negado o exceptuado, siempre que se trate de las circunstancias legítimas y necesarias y los derechos particulares o privados consagrados en el artículo 18 de la Ley 1712 de 2014. (Ley 1712 de 2014, art 6).

Información Pública Reservada

Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, es exceptuada de acceso a la ciudadanía por daño a intereses públicos y bajo cumplimiento de la totalidad de los requisitos consagrados en el artículo 19 de la Ley 1712 de 2014. (Ley 1712 de 2014, art 6)

Plan de continuidad del negocio

Plan orientado a permitir la continuación de las principales funciones misionales o del negocio en el caso de un evento imprevisto que las ponga en peligro. (ISO/IEC 27000).

Plan de tratamiento de riesgos

Documento que define las acciones para gestionar los riesgos de seguridad de la información inaceptables e implantar los controles necesarios para proteger la misma. (ISO/IEC 27000).

Privacidad

En el contexto de este documento, por privacidad se entiende el derecho que tienen todos los titulares de la información en relación con la información que involucre datos personales y la información clasificada que estos hayan entregado o esté en poder de la entidad en el marco de las funciones que a ella le compete realizar y que generan en las

entidades destinatarias del Manual de GEL la correlativa obligación de proteger dicha información en observancia del marco legal vigente.

Responsabilidad Demostrada

Conducta desplegada por los Responsables o Encargados del tratamiento de datos personales bajo la cual a petición de la Superintendencia de Industria y Comercio deben estar en capacidad de demostrarle a dicho organismo de control que han implementado medidas apropiadas y efectivas para cumplir lo establecido en la Ley 1581 de 2012 y sus normas reglamentarias.

Responsable del Tratamiento de Datos

Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, decida sobre la base de datos y/o el Tratamiento de los datos. (Ley 1581 de 2012, art 3).

Riesgo

Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias. (ISO/IEC 27000).

Seguridad de la información

Preservación de la confidencialidad, integridad, y disponibilidad de la información. (ISO/IEC 27000).

Sistema de Gestión de Seguridad de la Información SGSI

Conjunto de elementos interrelacionados o interactuantes (estructura organizativa, políticas, planificación de actividades, responsabilidades, procesos, procedimientos y recursos) que utiliza una organización para establecer una política y unos objetivos de seguridad de la información y alcanzar dichos objetivos, basándose en un enfoque de gestión y de mejora continua. (ISO/IEC 27000).

Titulares de la información

Personas naturales cuyos datos personales sean objeto de Tratamiento. (Ley 1581 de 2012, art 3).

Trazabilidad

Cualidad que permite que todas las acciones realizadas sobre la información o un sistema de tratamiento de la información sean asociadas de modo inequívoco a un individuo o entidad. (ISO/IEC 27000).

OBJETIVO

Controlar y minimizar los riesgos asociados a los procesos tecnológicos existentes, en el Instituto Nacional de Salud, con el fin de salvaguardar los activos de información, el manejo de medios, control de acceso y gestión de usuarios.

Objetivos Específicos

1. Determinar el alcance del plan de gestión de riesgos de la seguridad y privacidad de la información.
2. Definir los principales activos a proteger en la alcaldía.
3. Identificar las principales amenazas que afectan a los activos.

RECURSOS

- **Humano**: Gerente General, Líderes del Proceso, Profesional 3 Tecnología, Personal Externo
- **Físico:** Firewall, PC y equipos de comunicación
- **Financieros**: $17.000.000 (Diecisiete Millones)

RESPONSABLES

Gerente General
Líderes del Proceso
Profesionales Tecnología

METODOLOGÍA DE IMPLEMENTACIÓN

Para llevar a cabo la implementación El Plan de Tratamiento de Riesgos en el Instituto Nacional de Salud, se divide en varias fases como son:

FASE II: ESTABLECIMIENTO DEL SGSI		
DISEÑO DEL PROCESO DE GESTIÓN DE INCIDENTES DE SEGURIDAD		
Objetivo	**Actividades**	**Productos**
Definir y documentar formalmente el proceso de gestión de incidentes del SGSI	Proponer el modelo del proceso para la gestión de incidentes, incorporando los recursos existentes en el INS, como canales de comunicación, mesas de ayuda, políticas y procedimientos relacionados con la continuidad de negocio: • Revisión del proceso actual de manejo de incidentes • Identificación de mejores prácticas (ITIL, DRII, FIRST)	Procedimiento para la gestión de incidentes de seguridad de la información
	• Desarrollo de procedimientos, instructivos y guías relacionados. • Elaboración del plan de implementación del modelo gestión de incidentes • Aprobación y divulgación El procedimiento deberá incluir como mínimo los siguientes ítems: • Objetivos. • Roles y responsabilidades. • Procedimiento de gestión de incidentes: preparación, identificación, contención, remediación, recuperación y lecciones aprendidas. • Mejora continua del proceso. • Métricas e indicadores. • Anexo con el procedimiento específico para diez (10) tipos de incidentes específicos a acordar entre las partes, entre las cuales se tienen: phishing, ransomware, denegación de servicio, entre otras.	

FASE II: ESTABLECIMIENTO DEL SGSI		
DEFINICION E IMPLEMENTACIÓN DEL MODELO DE MEDICIÓN DEL SGSI		
Objetivo	**Actividades**	**Productos**
Crear, definir e implementar los indicadores (métricas) adecuados para medir la madurez, eficiencia, eficacia, implantación o impacto de controles de seguridad de la información Se deberá tener como referencia la norma ISO 27004:2016	Identificar cuáles son las métricas e indicadores adecuadas que resulten útiles para el seguimiento de los resultados y la dirección de los recursos y la demostración de evidencia de gestión de riesgos. El modelo deberá contener como mínimo los siguientes elementos: • • Indicadores para la medición del SGSI y MPSI.	• Definición de indicadores de gestión, como mínimo deberán ser 15 indicadores. • Modelo de medición del SGSI y MPSI. • Informe de la medición.
	• Indicadores de la efectividad de los principales controles de seguridad. • Fichas técnicas de los indicadores (fuentes de datos, responsables, periodicidad, meta, etc.) • Procedimiento de medición. análisis y evaluación de las mediciones (acciones correctivas) • Roles y responsabilidades. • Seguridad de los registros Una vez aprobado el modelo se deberá ejecutar el procedimiento de medición abarcando todos los indicadores, análisis y propuesta de las acciones correctivas a que haya lugar	•

FASE III: ANÁLISIS DE RIESGOS		
IDENTIFICACIÓN DE ACTIVOS DE INFORMACIÓN		
Objetivo	**Actividades**	**Productos**
Identificar los activos de información de los procesos de negocio INS incluidos en el alcance. Construir la matriz de clasificación de los activos de información de acuerdo con los requerimientos de confidencialidad definidos y establecer los requerimientos exigidos por la norma ISO27001:2013 y normas relacionadas ISO 27002 e ISO 27005	Realizar el levantamiento de las bases de datos de información personal basados en la guía de responsabilidad demostrada y la ley de protección de datos personales, para el reporte ante la Superintendencia de Industria y Comercio (SIC) cumpliendo con los lineamientos para su presentación Identificar los activos de información, según la ISO27005 se clasificación en dos tipos: **Primarios**: • Procesos y actividades del negocio • Información (Datos e Información Impresa)	• Inventario de activos de información. • Inventario de bases de datos personales.
	Apoyo: • Hardware (Equipos informáticos) • Software (Aplicaciones) • Redes de comunicaciones • Personal • Medios de Almacenamiento • Servicios de Terceros	•
	Identificar y describir los posibles impactos de seguridad que afectarían a la empresa o a los objetivos del negocio y que se deriven directamente de la divulgación de información sensitiva. Definir las reglas para medir los	•

FASE III: ANÁLISIS DE RIESGOS		
IDENTIFICACIÓN DE ACTIVOS DE INFORMACIÓN		
Objetivo	**Actividades**	**Productos**
	niveles de confidencialidad de los activos de información incluidos en el alcance Revisar los procesos vigentes en la organización incluidos dentro del alcance, para identificar previo a las entrevistas los posibles activos de información Identificar los activos de información que cada área genera, procesa o utiliza y los requerimientos de confidencialidad de los mismos. Depurar y consolidar la información recopilada generando el inventario de activos de información para identificar los activos críticos insumo para el análisis de riesgos y posterior tratamiento.	

FASE III: ANÁLISIS DE RIESGOS		
ANÁLISIS DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN		
Objetivo	**Actividades**	**Productos**
Elaborar el mapa de riesgos de la organización basada en los lineamientos establecidos en la norma ISO 31000 e ISO 27005:2008	En base al levantamiento de los activos de información se deberá proceder a ejecutar el análisis de riesgos, contemplando las siguientes actividades: • Identificación del Nivel de riesgo Aceptable. • Plan de tratamiento de Riesgos. • Presentación y socialización de resultados • Determinar la declaración de aplicabilidad, en concordancia con la cláusula 6.1.3 de ISO 27001 versión 2013.	Definición de la metodología de Análisis de riesgos de Seguridad de la Información Documento de análisis de riesgos que incluya identificación de amenazas y vulnerabilidades, Matriz de Riesgos del proceso. Plan de tratamiento de riesgos de seguridad de la información. Informe de Análisis de riesgos para los procesos definidos en el alcance. Declaración de aplicabilidad (SOA)

FASE IV: PRUEBAS DE SEGURIDAD HACKING ÉTICO Y PENETRACIÓN		
Objetivo	**Actividades**	**Productos**
Mediante estas pruebas se busca evidenciar las vulnerabilidades que existen dentro de la configuración física y lógica de los sistemas informáticos de la entidad.	**HACKING ÉTICO**: • Recolección de información. • Identificación de sistemas y servicios. • Identificación y verificación de vulnerabilidades. • Presentación informes de resultados. **Metodologías:** Realizar pruebas de Hacking Ético con el uso de la metodología OSSTMM v3. Realizar pruebas sobre aplicaciones Web con el uso de la metodología OWASP, como mínimo se deberán realizar las siguientes pruebas: • Ataque de inyección de código malicioso (XSS) • Autenticación y Gestión de Sesiones • Referencias inseguras a objetos directos • Configuración errónea de Seguridad • Redirecciones y reenvíos no validados **Herramientas:** Utilizar herramientas y Frameworks de trabajo reconocidas y que representen la manera de actuar por parte de un atacante real tales como: • Metasploit FrameWork	Informe final de Hacking Ético y las recomendaciones que se dan a conocer a la organización sobre las pruebas de hacking ético definidas en el alcance: • 54 servidores • 6 aplicaciones misionales • 3 aplicaciones administrativas • Hasta 4 dispositivos de seguridad perimetral con IP pública configurada Informe Técnico de Pruebas del análisis de vulnerabilidad y test intrusión Informe Ejecutivo de Pruebas del análisis de vulnerabilidad y test intrusión Informe con las posibles soluciones frente a las vulnerabilidades encontradas. Recomendaciones sobre aspectos a mejorar a nivel de cultura de seguridad.

FASE IV: PRUEBAS DE SEGURIDAD		
HACKING ÉTICO Y PENETRACIÓN		
Objetivo	**Actividades**	**Productos**
	• KALI Pentest FrameWork • Web Application Attack and Audit FrameWork • Tenable Nessus Professional Feed • Nmap	

ACTIVIDADES

1. Realizar Diagnóstico
2. Elaborar el Alcance del Plan del Tratamiento de Riesgo de Seguridad y Privacidad de la Información
4. Realizar la Identificación de los Riesgos con los líderes del Proceso.
   3.1. Entrevistar con los líderes del Proceso valorando el riesgo y el riesgo residual
5. Realizar Mapas de calor donde se ubican los riesgos
6. Plantear al plan de tratamiento de riego aprobado por los lideres

8. CUMPLIMIENTO DE IMPLEMENTACIÓN

De acuerdo a las fases mencionadas anteriormente, se describe a continuación los dominios que se deben desarrollar y los plazos de implementación de acuerdo a lo establecido por el Instituto Nacional de Salud.

Revisión y/o Modificación de la actual Política de Seguridad.
Aspectos organizativos de la seguridad de la información
Seguridad Ligada a los recursos humanos
Revisión del Control de acceso
Seguridad en la operativa
Seguridad en las telecomunicaciones
Gestión de Incidentes de Seguridad de la Información
Aspectos de seguridad de la información en la gestión de continuidad del negocio.

CRONOGRAMA

Av. Calle 26 No. 51- 20, Bogotá, D.C., Colombia
Conmutador: (1) 220 7700 Ext. 1703-1704
fax: 220 7700 Ext. 1283-1269
correo electrónico: contactenos@ins.gov.co
Página web: **www.ins.gov.co**
Línea gratuita nacional: 018000 113 400

ACTIVIDAD	Mayo	Junio	Julio	Agosto	Septiembre	Octubre	Noviembre	Diciembre

Radicación estuidos previos								
Definir y documentar formalmente el proceso de gestión de incidentes del SGSI								
Crear, definir e implementar los indicadores (métricas) adecuados para medir la madurez, eficiencia, eficacia, implantación o impacto de controles de seguridad de la información. Se deberá tener como referencia la norma ISO 27004:2016								
Identificar los activos de información de los procesos de negocio INS incluidos en el alcance.								
Construir la matriz de clasificación de los activos de información de acuerdo con los requerimientos de confidencialidad definidos y establecer los requerimientos exigidos por la norma ISO27001:2013 y normas relacionadas ISO 27002 e ISO 27005								
Elaborar el mapa de riesgos de la organización basada en los lineamientos establecidos en la norma ISO 31000 e ISO 27005:2008								
Mediante estas pruebas se busca evidenciar las vulnerabilidades que existen dentro de la configuración física y lógica de los sistemas informáticos de la entidad.								