INSTITUTO NACIONAL DE SALUD

PLAN DE 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

Glosario

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).

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).

Adware

Adware es un software, generalmente no deseado, que facilita el envío de contenido publicitario a un equipo.

Advertencia

Mensaje que comunica al usuario que una acción puede ocasionar u ocasionara la pérdida de datos del sistema del usuario.

Alarma

Sonido o señal visual que se activa cuando se produce una condición de error.

Alerta

Notificación automática de un suceso o un error.

Amenaza

Una amenaza informática es toda circunstancia, evento o persona que tiene el potencial de causar daño a un sistema en forma de robo, destrucción, divulgación, modificación de datos o negación de servicio (DoS).

Amenazas polimorfas

Las amenazas polimorfas son aquellas que tienen la capacidad de mutar y en las cuales cada instancia del malware es ligeramente diferente al anterior a este. Los cambios automatizados en el código realizados a cada instancia no alteran la funcionalidad del malware, sino que prácticamente inutilizan las tecnologías tradicionales de detección antivirus contra estos ataques.

Amenaza Externa

Amenaza que se origina fuera de una organización.

Amenaza Interna

Amenaza que se origina en una organización.

Analizador

Herramienta de configuración automatizada que analiza una red en busca de sistemas activos y actúa como guía durante el proceso de definición de los sistemas que desea supervisar y de las firmas de ataques que desea asociar con cada sistema.

Antispam

Antispam es un producto, herramienta, servicio o mejor práctica que detiene el spam o correo no deseado antes de que se convierta en una molestia para los usuarios. El antispam debe ser parte de una estrategia de seguridad multinivel.

Antivirus

Antivirus es una categoría de software de seguridad que protege un equipo de virus, normalmente a través de la detección en tiempo real y también mediante análisis del sistema, que pone en cuarentena y elimina los virus. El antivirus debe ser parte de una estrategia de seguridad estándar de múltiples niveles.

Aplicaciones engañosas

Las aplicaciones engañosas son programas que intentan engañar a los usuarios informáticos para que emprendan nuevas acciones que normalmente están encaminadas a causar la descarga de malware adicional o para que los usuarios divulguen información personal confidencial. Un ejemplo es el software de seguridad fraudulento, que también se denomina scareware.

Arquitectura de Seguridad

Conjunto de principios que describe los servicios de seguridad que debe proporcionar un sistema para ajustarse a las necesidades de sus usuarios, los elementos de sistema necesarios para implementar tales servicios y los niveles de rendimiento que se necesitan en los elementos para hacer frente a las posibles amenazas.

Ataques multi-etapas

Un ataque en múltiples etapas es una infección que normalmente implica un ataque inicial, seguido por la instalación de una parte adicional de códigos maliciosos. Un ejemplo es un troyano que descarga e instala adware.

Ataques Web

Un ataque Web es un ataque que se comete contra una aplicación cliente y se origina desde un lugar en la Web, ya sea desde sitios legítimos atacados o sitios maliciosos que han sido creados para atacar intencionalmente a los usuarios de ésta.

Autenticación

Garantía de que una parte de una transacción informática no es falsa. La autenticación normalmente lleva consigo el uso de una contraseña, un certificado, un número de identificación personal u otra información que se pueda utilizar para validar la identidad en una red de equipos.

Blacklisting o Lista Negra

La lista negra es el proceso de identificación y bloqueo de programas, correos electrónicos, direcciones o dominios IP conocidos maliciosos o malévolos.

Bot

Un bot es una computadora individual infectada con malware, la cual forma parte de una red de bots (botnet).

Botnet

Conjunto de equipos bajo el control de un bot maestro, a través de un canal de mando y control. Estos equipos normalmente se distribuyen a través de Internet y se utilizan para actividades malintencionadas, como el envío de spam y ataques distribuidos de negación de servicio. Las botnet se crean al infectar las computadoras con malware, lo cual da al atacante acceso a las máquinas. Los propietarios de computadoras infectadas generalmente ignoran que su máquina forma parte de una botnet, a menos que tengan software de seguridad que les informe acerca de la infección.

Caballo de Troya

Son un tipo de código malicioso que parece ser algo que no es. Una distinción muy importante entre troyanos y virus reales es que los troyanos no infectan otros archivos y no se propagan automáticamente. Los caballos de troya tienen códigos maliciosos que cuando se activan causa pérdida, incluso robo de datos. Por lo general, también tienen un componente de puerta trasera, que le permite al atacante descargar amenazas adicionales en un equipo infectado. Normalmente se propagan a través de descargas inadvertidas, archivos adjuntos de correo electrónico o al descargar o ejecutar voluntariamente un archivo de Internet, generalmente después de que un atacante ha utilizado ingeniería social para convencer al usuario de que lo haga.

Certificado

Los sistemas criptográficos utilizan este archivo como prueba de identidad. Contiene el nombre del usuario y la clave pública.

Crimeware

Software que realiza acciones ilegales no previstas por un usuario que ejecuta el software. Estas acciones buscan producir beneficios económicos al distribuidor del software.

Ciberdelito

El ciberdelito es un delito que se comete usando una computadora, red o hardware.
La computadora o dispositivo puede ser el agente, el facilitador o el objeto del delito.
El delito puede ocurrir en la computadora o en otros lugares.

Contraseña

Cadena exclusiva de caracteres que introduce un usuario como código de identificación para restringir el acceso a equipos y archivos confidenciales. El sistema compara el código con una lista de contraseñas y usuarios autorizados. Si el código es correcto, el

sistema permite el acceso en el nivel de seguridad aprobado para el propietario de la contraseña.

Cuarentena

Aislar archivos sospechosos de contener algún virus, de modo que no se pueden abrir ni ejecutar.

Encriptación

La encriptación es un método de cifrado o codificación de datos para evitar que los usuarios no autorizados lean o manipulen los datos. Sólo los individuos con acceso a una contraseña o clave pueden descifrar y utilizar los datos. A veces, el malware utiliza la encriptación para ocultarse del software de seguridad. Es decir, el malware cifrado revuelve el código del programa para que sea difícil detectarlo.

Exploits o Programas intrusos

Los programas intrusos son técnicas que aprovechan las vulnerabilidades del software y que pueden utilizarse para evadir la seguridad o atacar un equipo en la red.

Filtración de datos

Una filtración de datos sucede cuando se compromete un sistema, exponiendo la información a un entorno no confiable. Las filtraciones de datos a menudo son el resultado de ataques maliciosos, que tratan de adquirir información confidencial que puede utilizarse con fines delictivos o con otros fines malintencionados

Firewall

Un firewall es una aplicación de seguridad diseñada para bloquear las conexiones en determinados puertos del sistema, independientemente de si el tráfico es benigno o maligno. Un firewall debería formar parte de una estrategia de seguridad estándar de múltiples niveles.

Grooming

Es una nueva forma de acoso y abuso hacia niños y jóvenes que se ha venido popularizando con el auge de las TIC, principalmente los chats y redes sociales. Inicia con una simple conversación virtual, en la que el adulto se hace pasar por otra persona, normalmente, por una de la misma edad de víctima con el fin de

Gusanos

Los gusanos son programas maliciosos que se reproducen de un sistema a otro sin usar un archivo anfitrión, a diferencia de un Virus.

Ingeniería Social

Método utilizado por los atacantes para engañar a los usuarios informáticos, para que realicen una acción que normalmente producirá consecuencias negativas, como la descarga de malware o la divulgación de información personal. Los ataques de phishing con frecuencia aprovechan las tácticas de ingeniería social.

Keystroke Logger o Programa de captura de teclado (Keylogger)

Es un tipo de malware diseñado para capturar las pulsaciones, movimientos y clics del teclado y del ratón, generalmente de forma encubierta, para intentar robar información personal, como las cuentas y contraseñas de las tarjetas de crédito.

Malware

El malware es la descripción general de un programa informático que tiene efectos no deseados o maliciosos. Incluye virus, gusanos, troyanos y puertas traseras. El malware a menudo utiliza herramientas de comunicación populares, como el correo electrónico y la mensajería instantánea, y medios magnéticos extraíbles, como dispositivos USB, para difundirse. También se propaga a través de descargas inadvertidas y ataques a las vulnerabilidades de seguridad en el software. La mayoría del malware peligroso actualmente busca robar información personal que pueda ser utilizada por los atacantes para cometer acciones delictivas.

Mecanismo de propagación

Un mecanismo de propagación es el método que utiliza una amenaza para infectar un sistema.

Negación de servicio (DoS)

La negación de servicio es un ataque en el que el delincuente intenta deshabilitar los recursos de una computadora o red para los usuarios. Un ataque distribuido de negación de servicio (DDoS) es aquel en que el atacante aprovecha una red de computadoras distribuidas, como por ejemplo una botnet, para perpetrar el ataque.

Pharming

Método de ataque que tiene como objetivo redirigir el tráfico de un sitio Web a otro sitio falso, generalmente diseñado para imitar el sitio legítimo. El objetivo es que los usuarios permanezcan ignorantes del re-direccionamiento e ingresen información personal, como la información bancaria en línea, en el sitio fraudulento.

Phishing

Método más utilizados por delincuentes cibernéticos para estafar y obtener información confidencial de forma fraudulenta como puede ser una contraseña o información detallada sobre tarjetas de crédito u otra información bancaria de la víctima.

Redes punto a punto (P2P)

Red virtual distribuida de participantes que hacen que una parte de sus recursos informáticos estén a disposición de otros participantes de la red, todo sin necesidad de servidores centralizados. Las redes puntos a punto son utilizadas para compartir música, películas, juegos y otros archivos. Sin embargo, también son un mecanismo muy común para la distribución de virus, bots, spyware, adware, troyanos, rootkits, gusanos y otro tipo de malware.

Riesgo

El riesgo es el efecto de la incertidumbre sobre los objetivos.

Rootkits

Componente de malware que utiliza la clandestinidad para mantener una presencia persistente e indetectable en un equipo. Las acciones realizadas por un rootkit, como la instalación y diversas formas de ejecución de códigos, se realizan sin el conocimiento o consentimiento del usuario final.

Los rootkits no infectan las máquinas por sí mismos como lo hacen los virus o gusanos, sino que tratan de proporcionar un entorno indetectable para ejecutar códigos maliciosos. Los atacantes normalmente aprovechan las vulnerabilidades en el equipo seleccionado o utilizan técnicas de ingeniería social para instalar manualmente los rootkits. O, en algunos casos, los rootkits pueden instalarse automáticamente al ejecutarse un virus o gusano o incluso simplemente al navegar en un sitio Web malicioso.

Sistema de detección de intrusos

Un sistema de detección de intrusos es un servicio que monitorea y analiza los eventos del sistema para encontrar y proporcionar en tiempo real o casi real advertencias de

intentos de acceso a los recursos del sistema de manera no autorizada. Es la detección de ataques o intentos de intrusión, que consiste en revisar registros u otra información disponible en la red. Un sistema de detección de intrusos debe ser parte de una estrategia de seguridad estándar de múltiples niveles.

Sistema de prevención de intrusos

Un sistema de prevención de intrusos es un dispositivo (hardware o software) que supervisa las actividades de la red o del sistema en busca de comportamiento no deseado o malicioso y puede reaccionar en tiempo real para bloquear o evitar esas actividades. Un sistema de prevención de intrusos debe ser parte de una estrategia de seguridad estándar de múltiples niveles.

Spam

También conocido como correo basura, el spam es correo electrónico que involucra mensajes casi idénticos enviados a numerosos destinatarios. Un sinónimo común de spam es correo electrónico comercial no solicitado (UCE). El malware se utiliza a menudo para propagar mensajes de spam al infectar un equipo, buscar direcciones de correo electrónico y luego utilizar esa máquina para enviar mensajes de spam. Los mensajes de spam generalmente se utilizan como un método de propagación de los ataques de phishing

Spyware o Software Espía

El software espía consta de un paquete de software que realiza un seguimiento y envía información confidencial o personal a terceros. La información personal es información que puede atribuirse a una persona específica, como un nombre completo. La información confidencial incluye datos que la mayoría de las personas no desearía compartir con otras, como detalles bancarios, números de tarjetas de créditos y contraseñas. Terceros puede hacer referencia a sistemas remotos o partes con acceso local.

Virus

Programa informático escrito para alterar la forma como funciona una computadora, sin permiso o conocimiento del usuario. Un virus debe cumplir con dos criterios:

Debe ejecutarse por sí mismo: generalmente coloca su propio código en la ruta de ejecución de otro programa.

Debe reproducirse: por ejemplo, puede reemplazar otros archivos ejecutables con una copia del archivo infectado por un virus. Los virus pueden infectar computadores de escritorio y servidores de red.

Muchos de los virus actuales están programados para operar sigilosamente la computadora del usuario con el fin de robar información personal y utilizarla para cometer delitos. Otros menoscaban el equipo dañando los programas, eliminando archivos o volviendo a formatear el disco duro. Aún existen otros que no están diseñados para causar daño, aunque simplemente se reproducen y hacen manifiestan su presencia presentando mensajes de texto, video y audio, aunque este tipo de ataques de notoriedad no son tan comunes, puesto que los autores de virus y demás malware tiene como fin obtener ganancias ilegales.

Vulnerabilidad

Una vulnerabilidad es un estado viciado en un sistema informático (o conjunto de sistemas) que afecta las propiedades de confidencialidad, integridad y disponibilidad de los sistemas. Las vulnerabilidades pueden hacer lo siguiente:

b) Permitir que un atacante ejecute comandos como otro usuario
c) Permitir a un atacante acceso a los datos, lo que se opone a las restricciones específicas de acceso a los datos
d) Permitir a un atacante hacerse pasar por otra entidad
e) Permitir a un atacante realizar una negación de servicio

Objetivo

La seguridad y privacidad de la información se encamina en mantener un ambiente razonablemente seguro, alineado a la misión del Instituto Nacional de Salud y que permita proteger los activos de información de la misma, así como el uso adecuado de los recursos y gestión del riesgo, con el fin de emplear los principios de disponibilidad, integridad y confidencialidad de la información y el aseguramiento de la continuidad del negocio.

Objetivos Específicos

- Sensibilizar y capacitar a los servidores públicos, proveedores y partes interesadas acerca del Sistema de Gestión de Seguridad de la Información y el Modelo de Seguridad y Privacidad de la Información, de Gobierno Digital.

- Proteger y hacer diagnóstico de los activos de información del Instituto Nacional de Salud con base en los principios de confidencialidad, integridad y disponibilidad.

- Administrar, administrar y monitorear los riesgos de seguridad de la información para mantenerlos en niveles aceptables.

- Implementar acciones correctivas y de mejora para el Sistema de Gestión de Seguridad de la Información y el Modelo de Seguridad y Privacidad de la Información, de Gobierno Digital.

Alcance

Realizar las fases de análisis de brecha, establecimiento del Sistema de Gestión de Seguridad de la Información (SGSI), análisis de riesgos, pruebas de seguridad, plan estratégico de seguridad de la información, sensibilización y capacitación para la implementación del Modelo de Seguridad y Privacidad de la Información (MSPI) conforme a los lineamientos del Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC) y la Estrategia de Gobierno en Línea, contemplando la revisión, actualización de la documentación y el levantamiento de los riesgos de todos los procesos de la institución para garantizar la confidencialidad, integridad y disponibilidad de la información generada en el Instituto Nacional de Salud.

POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Que la Ley 1341 de 2009 "por la cual se definen principios y conceptos sobre la seguridad de la informaci6n y la organización de las tecnologías de la información y las comunicaciones - TIC- se crea la agencia nacional de espectro y se dictan otras disposiciones", señala en su artículo 2°, como principios orientadores y aspectos fundamentales para la promoción de la libre competencia y el comercio electrónico, lo siguiente: la protección a los derechos de los usuarios de las TIC, el acceso y uso de las TIC, la garantía de los derechos de los ciudadanos y la masificación del Gobierno Digital. Que el Decreto 1078 de 2015 en el artículo 2.2.9.1.1.1. establece como objeto "Definir los lineamientos, instrumentos y plazos de la estrategia de Gobierno en línea para garantizar el máximo aprovechamiento de las Tecnologías de la Información y las Comunicaciones, con el fin de contribuir con la construcci6n de un Estado abierto, más eficiente, más transparente y más participativo y que preste mejores servicios con la colaboraci6n de toda la sociedad". Que el Ministerio de Tecnologías de la Información y las Comunicaciones - MinTIC a través de la Dirección de Estándares y Arquitectura de TI y la Subdirección de Seguridad y Privacidad de TI, dando cumplimiento a sus funciones; publico el Modelo de Seguridad y Privacidad de la Información (MSPI), el cual se encuentra alineado con el Marco de Referencia de Arquitectura TI y soporta transversalmente los otros componentes.

El Objeto de la política, resolución 1463 de octubre de 2017, La Dirección General del Instituto Nacional de Salud, entendiendo la importancia de una adecuada gestión de la información, se ha comprometido con la implementaci6n de un sistema de gestión de seguridad de la información buscando establecer un marco de confianza en el ejercicio de sus deberes con el Estado y los ciudadanos, todo enmarcado en el estricto cumplimiento de las leyes y en concordancia con la misión y visión de la entidad. Para el Instituto Nacional de Salud la protección de la información busca la disminucion del impacto generado sobre sus actives, por los riesgos identificados de manera sistemática con

objeto de mantener un nivel de exposición que permita responder por la integridad, confidencialidad y la disponibilidad de la misma, acorde con las necesidades de los diferentes grupos de interés identificados.

El Instituto Nacional de Salud, mediante la Política de seguridad de información da cumplimiento a los lineamientos de la Planeación Estratégica de la entidad en concordancia con su misión, visión, objetivos y para ello debe tener en cuenta:

a) Gestionar el riesgo de los procesos estratégicos, misionales, de apoyo y de evaluación de la entidad.
b) Cumplir con los principios de seguridad de la información:

• **CONFIDENCIALIDAD**: la información debe ser accesible solo a aquellas personas autorizadas.
• **INTEGRIDAD**: la información y sus métodos de procesamiento deben ser completos y exactos.
• **DISPONIBILIDAD**: la información y los servicios deben estar disponible cuando se le requiera.

c) Mantener la confianza de los funcionarios, contratistas y terceros.
d) Mantener y Mejorar el sistema de gestión de seguridad de la información, cumpliendo con el ciclo PHVA
e) Proteger los activos de información.
f) Establecer las políticas, procedimientos e instructivos en materia de seguridad de la información.
g) Fortalecer la cultura de seguridad de la información en los funcionarios, terceros, aprendices, practicantes y clientes del INS. h) Proteger la información y los activos tecnológicos de la institución.
i) Adquirir un compromiso de concientización para que todos los funcionarios, contratistas y practicantes del INS sobre el uso adecuado de los activos de información puestos a su disposición para la realización de las funciones y actividades.
j) Dar cumplimiento a los lineamientos de la Estrategia de Gobierno en Digital respecto a la Seguridad de la Información.
k) Garantizar la continuidad del negocio frente a incidentes Brindar capacitaciones para el fortalecimiento de cambio de cultura.
L)Realizar campañas de sensibilización

Alcance

Esta política aplica a todo el Instituto Nacional de Salud, sus funcionarios, contratistas, terceros, colaboradores y ciudadana en general, así como a todos los activos de información, servicios, procesos, las tecnologías de información incluida el hardware y el software, instalaciones imagen perceptual y demás herramientas utilizadas por la Organización en el ejercicio de sus funciones.

Nivel de Cumplimiento

Todas las personas incluidas en artículo anterior deberán cumplir la política de manera obligatoria, en un 100%, sin perjuicio de las sanciones a que haya lugar.

Las políticas específicas de la Seguridad de la Información establecidas por el lNS son:

1. Definir, implementar, operar y mejorar de forma continua un Sistema de Gestión de Seguridad de la Información, soportado en lineamientos claros alineados a las necesidades del negocio, y a los requerimientos regulatorios que le aplican a su naturaleza. De igual manera las responsabilidades frente a la seguridad de la informaci6n serán definidas, compartidas, publicadas y aceptadas por cada uno de los empleados, contratistas o terceros.

2. Proteger la información generada, procesada 0 resguardada por los procesos estratégicos, misionales, de apoyo y de evaluaci6n, y garantizara su fiabilidad, integridad y disponibilidad por medio de la infraestructura tecnológica y los procesos y herramientas utilizadas, so pena de las sanciones que implican su incumplimiento.

3. Salvaguardar la información creada, procesada, transmitida 0 resguardada por sus procesos de negocio, con el fin de minimizar impactos financieros, operativos 0 legales debido a un uso incorrecto de es para ello es fundamental la aplicación de controles de acuerdo con la clasificación de la información de su propiedad 0 en custodia.

4. Limitar el acceso a los activos de información dependiendo de su clasificación siguen lo establecido en el marco de la normatividad.

5. Proteger las instalaciones físicas para controlar el acceso de personas no autorizadas a las áreas restringidas, con el fin de resguardar la información que se encuentra en ellas.

6. Controlar la operación de sus procesos de negocio garantizando la seguridad de los recursos tecnológicos y las redes de datos.

7. Garantizar el mantenimiento y seguridad de su infraestructura en donde se almacenen los Sistemas de Información para garantizar su ciclo de vida y los pilares de la seguridad de la información.

8. Evaluar a sus procedimientos, controles e infraestructura con el fin de detectar debilidades y riesgos asociados a la planta física en pro de una mejora efectiva en su modele de seguridad.

9. Proteger los datos personales recolectados en ejercicio de sus actividades como Autoridad Científico y Técnica del orden nacional, en el marco de nuestras competencias y de acuerdo con la Ley 1581 de 2012 y la Ley 1755 de 2015 0 las normas que la modifiquen o adicionen.

10. Preservar la información a la que tienen acceso los funcionaros, contratistas y colaboradores del Instituto Nacional de Salud y en consecuencia, incluirá clausulas en los contratos o convenios, o suscribirá los actos jurídicos necesarios para la protección de la información de acuerdo con los lineamientos dados por la Oficina Asesora Jurídica y el Comité de Propiedad Intelectual.

11. Velar por la concientización de los funcionarios, contratistas y terceros con respecto a la importancia y el cumplimiento de los lineamientos definidos a través del presente acto administrativa.

12. Informar a los terceros sobre la presente política de Seguridad de la Información y velar por su observancia en todos los actos jurídicos que suscriban con la Organización en los tramites que realicen frente a la misma de acuerdo con nuestras funciones.

13. Implementar los controles necesarios para dar manejo a los riesgos detectados y proveerá un nivel de protección de la información apropiado y consistente.

14. Administrar controles físicos y loticos para preservar y mantener seguras las áreas físicas y lógicas clasificadas como públicas y restringidas que sean utilizadas para la gestión, almacenamiento y procesamiento de la información.

15. Emitir mecanismos de control de acceso tales como puertas de seguridad donde se requieran, sistemas de alarmas, control biométrico, sistemas de detección y extinción de incendios, control de inundaciones, alarmas para detectar irregularidades en el desarrollo de las actividades, apartar líquidos inflamables y demás medidas que se deban tomar para la protección de la información de la Entidad. Las puertas de las oficinas y diferentes áreas de la entidad deben permanecer cerradas y aseguradas cuando las mismas se encuentren desatendidas sin personal de la entidad dentro de ellas.

16. Otorgar claves de acceso los sistemas de información, equipos de compute, alarmas, cajas fuertes entre otros unicarnente a personal autorizado, salvo las situaciones de emergencia que se puedan presentar.

17. Restringir el acceso a los funcionarios de la Entidad, contratistas, colaboradores y terceros, solo a áreas a las cuales tengan la debida autorización.

18. Custodiar en todo momento y sin excepción a todos los visitantes que ingresen a la Entidad, durante su permanencia en las instalaciones del INS.

19. Velar por la seguridad de la información de los equipos de compute que salgan de la institución, 10 cual se realizar unicarnente con autorización del Jefe inmediato.

20. Utilizar la documentaci6n física generada, recibida y en general, manipulada por los funcionarios, unicarnente para el ejercicio de las responsabilidades de la Entidad de acuerdo con las funciones del servidor público y actividades que realice el contratista y tercero, so pena del inicio de las acciones a que haya lugar, en concordancia con la normatividad.

21. Tomar las medidas a que haya lugar, una vez se tenga conocimiento de incidentes de seguridad 0 violaci6n a las medidas que han sido tomadas para garantizar la seguridad de la informaci6n.

22. Bloquear el acceso a las páginas de contenido para adultos, mensajería instantánea y demás páginas que no sean de uso corporativo mediante el uso de servidor proxy, firewall 0 el software institucional.

23. Definir y Divulgar el procedimiento para la realización copias de seguridad de la Informaci6n y velara por su archivo y custodia de acuerdo con la normatividad.

24. Realizar de manera periódica pruebas de funcionamiento de las copias de seguridad para garantizar su correcta recuperaci6n en el caso de ser necesario.

25. Instalar y desinstalar software y programas de cómputo los cuales en todo caso contaran con las licencias de uso respectivas. El funcionario de la entidad no podrá instalar ningún programa sin la autorización respectiva y de acuerdo con sus funciones. 10 anterior se realiza a través de la Oficina TIC.

26. Tomar las demás medidas a que haya lugar, en desarrollo y estandarizaci6n de la presente política de Seguridad de la Informaci6n.

Responsabilidades Especificas frente a la Seguridad de la Información y al Sistema de Gestión de Seguridad de la Información.

Responsables.

El Responsable Institucional de la implementaci6n, aplicación, seguimiento y demás actividades derivadas para la estandarización de la presente Política, es el Jefe de la Oficina de Tecnologías de Información y Comunicaciones, y quien haga sus veces, el grupo de soporte tecnológico de la secretaria general, propietarios de la informaci6n, funcionarios, contratistas y practicantes usuarios de la información, sin perjuicio de las funciones del Comité Institucional de Desarrollo Administrativo y la Oficina de Control interno.

I. RESPONSABILIDADES DE LA OFICINA DE Tecnologías DE LA INFORMACION

a) Implantar, mantener y divulgar las políticas y procedimientos de tecnología, incluida esta política de seguridad de información, el uso de los servicios tecnológicos en toda la institución de acuerdo a las mejores prácticas y lineamientos de la Dirección General del Instituto y directrices del Gobierno.
b) Salvaguardar la información que reposa en los diferentes sistemas de información, bases de dalos y aplicativos de la institución.
c) Informar de los eventos que estén en contra de la seguridad de la información y de la infraestructura tecnológica de la institución a la Dirección General, las diferentes Direcciones y Jefaturas del Instituto Nacional de Salud, así como a los entes de control e investigación que tienen injerencia sobre la institución.
d) Proporcionar medidas de seguridad físicas, loicas y procedimentales para la protecci6n de la información digital del Instituto.
e) Aplicar y hacer cumplir la Política de Seguridad de la Información y sus componentes.
f) Administrar las reglas y atributos de acceso a los equipos de compute, sistemas de información, aplicativos y dernas fuentes de información al servicio del Instituto Nacional de Salud.
g) Analizar, aplicar y mantener los controles de seguridad implementados para asegurar los dalos e información gestionados en la institución.
h) Resolver de común acuerdo con las áreas y los propietarios de la información los conflictos que se presenten por la propiedad de la información al interior del Instituto.
i) Habilitar/Deshabilitar el reconocimiento y operación de Dispositivos de Almacenamiento externo de acuerdo con las directrices emitidas de parte de la Dirección General y las diferentes direcciones.

j) Implementar los mecanismos de controles necesarios y pertinentes para verificar el cumplimiento de la presente política.

RESPONSABILIDADES DEL AREA DE SOPORTE TECNOLOGICO DE LA SECRETARIA GENERAL

a) Garantizar la disponibilidad de los servicios y así mismo programar 0 informar a todos los usuarios.
b) Resolver cualquier problema de mantenimiento que pueda afectar la normal prestación de los mismos; así como gestionar su acceso de acuerdo a las solicitudes recibidas de las diferentes Direcciones, Jefaturas 0 Coordinaciones siguiendo el procedimiento establecido. c) Establecer, mantener y divulgar las políticas y procedimientos de los servicios de tecnología, incluidos todos los capítulos que hacen parte de esta Política, en toda la institución de acuerdo a las mejores prácticas y directrices de la Entidad y del Gobierno. d) Determinar las estrategias para el mejoramiento continuo del servicio tecnológico, la optimización de los recursos tecnológicos, las mejoras en los sistemas de información con miras a un gobierno de tecnologías consolidado. e) Brindar el soporte necesario a los usuarios a través del apoyo del Recurso Humano y los diversos canales de apoyo y ayuda que se han implementados en el INS.

RESPONSABILIDADES DE LOS PROPIETARIOS DE LA INFORMACION

a) Son propietarios de la información cada uno de los Directores, así como los jefes de las oficinas donde se genera, procesa y mantiene información, en cualquier medio, propia del desarrollo de sus actividades.
b) Valorar y clasificar la información que está bajo su administración y/o generación.
c) Autorizar, restringir y delimitar a los dernas usuarios de la institución el acceso a la información de acuerdo a los roles y responsabilidades de los diferentes funcionarios, contratistas y practicantes que por sus actividades requieran acceder a consultar, crear y modificar parte de la totalidad de la información.
d) Determinar los tiempos de retención de la informaci6n en conjunto con el grupo de Gestión Documental y Correspondencia y las áreas que se encarguen de su protección y almacenamiento de acuerdo a las determinaciones y políticas de la entidad como de los entes externo os y las normas y leyes vigentes.
e) Determinar y evaluar de forma permanente los riesgos asociados a la información, así como los controles implementados para el acceso y gestión de la administración comunicando cualquier anomalía y mejora tanto a los usuarios como a los custodios de la misma.
f) Acoger e informar los requisitos de esta política a todos los funcionarios, contratistas y practicantes en las diferentes dependencias del Instituto.

RESPONSABILIDADES DE LOS FUNCIONARIOS, CONTRATISTAS Y PRACTICANTES USUARIOS DE LA INFORMACION

a) Utilizar solamente la informaci6n necesaria para llevar a cabo las funciones que le fueron asignadas, de acuerdo con los permisos establecidos 0 aprobados en el Manual de Funciones, Código Disciplinario Único Ley 734 de 2002 0 Contrato.

2. PLAN DE IMPLEMENTACIÓN DE LA SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Este componente de seguridad y privacidad de la información, exigido por el Manual de Gobierno en línea requiere como mínimo:

- Diagnóstico de Seguridad y Privacidad Plan de Seguridad y Privacidad de la Información: Busca determinar el estado actual del nivel de seguridad y privacidad de la información y de los sistemas de información
- Plan de Seguridad y Privacidad de la Información: Busca generar un plan de seguridad y privacidad alineado con el propósito misional.
- Gestión de riesgos de seguridad y privacidad de la información: Busca proteger los derechos de los usuarios de la entidad y mejorar los niveles de confianza en los mismos a través de la identificación, valoración, tratamiento y mitigación de los riesgos de los sistemas de información.
- Evaluación del desempeño: Busca hacer las mediciones necesarias para calificar la operación y efectividad de los controles, estableciendo niveles de cumplimiento y de protección de los principios de seguridad y privacidad de la información.
- Que, según la evaluación reportada a marzo de 2017, el avance de la entidad en el componente de seguridad y privacidad de la información es del 49%, encontrándose en un Nivel Intermedio, identificándose la necesidad de avanzar en la implementación del plan de tratamiento de riesgos de seguridad en todos los procesos de la entidad.

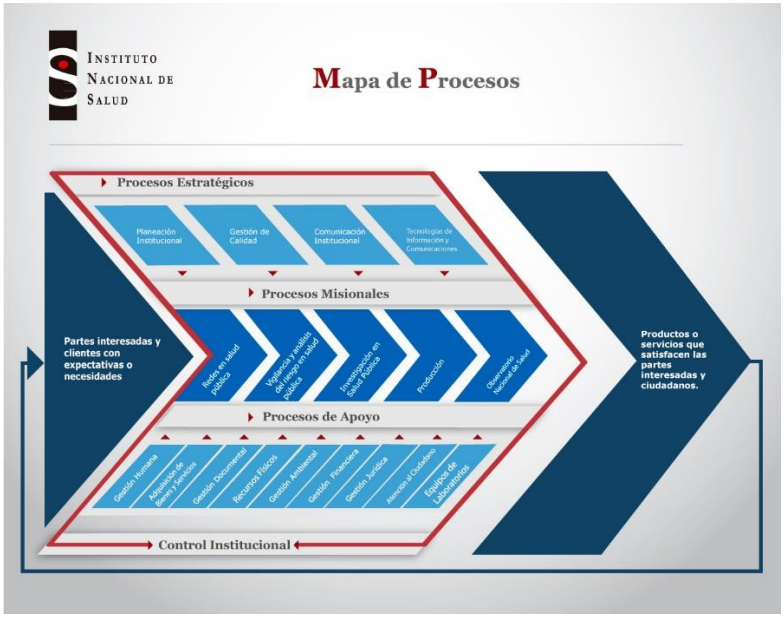
Que el Instituto Nacional de Salud, para cumplir con su misión y facilitar los trámites y servicios con los usuarios internos y externos y el acceso a la información viene desarrollando una serie de sistemas de información misionales y administrativos en ambiente Web, mediante los cuales se recoge información del orden Nacional y territorial y que para garantizar la disponibilidad, confidencialidad e integridad de la información, el INS, viene desarrollando actividades encaminadas a la implementación del modelo de seguridad y privacidad de la información (MSPI). La confidencialidad, integridad y disponibilidad de la información sensible son elementos esenciales para lograr los objetivos de la entidad.

Estos sistemas de información pueden estar expuestos a amenazas, como virus informáticos, o hacking, entre otros, pero también a riesgos de sufrir incidentes de seguridad causados voluntaria o involuntariamente desde dentro de la entidad o los causados accidentalmente por fallas técnicas y desastres naturales, por lo que es necesario continuar con la implementación del modelo de seguridad y privacidad de la información (MSPI), debido a que este sistema ayuda a la entidad a gestionar de manera eficaz la seguridad de la información; evaluando riesgos que afectan a la entidad, con el objetivo de definir y aplicar medidas, procesos y procedimientos para el apropiado control, tratamiento y mejora continua.

Se tendrán en cuenta todos los procesos de la entidad compuestos por nueve (9) procesos de apoyo, cinco (5) procesos estratégicos y cinco (5) misionales, es necesario realizar el levantamiento de los riesgos de seguridad en estos procesos y definir el plan de tratamiento de los mismos, para garantizar su confidencialidad, integridad y disponibilidad de la información que administran los mismos.

MAPA DE PROCESOS:

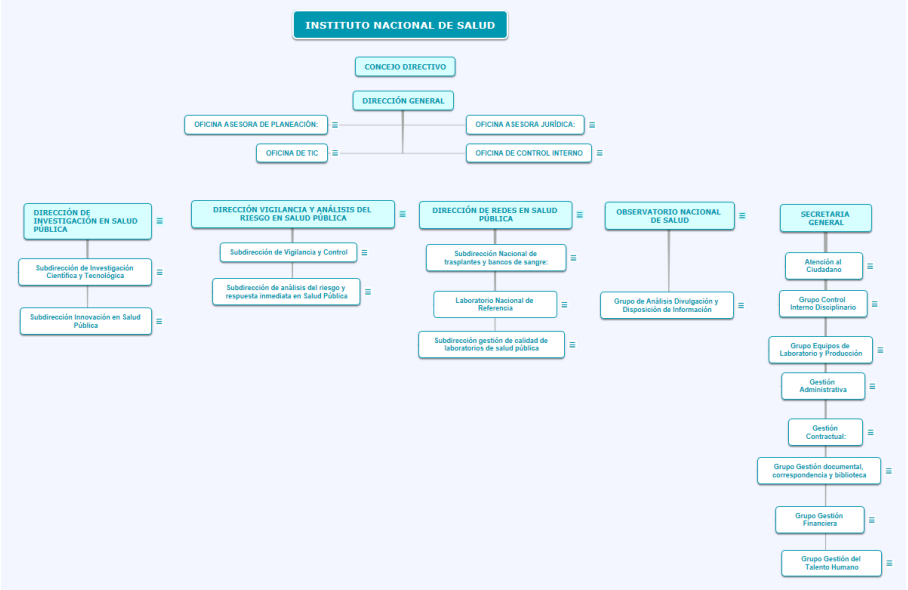
De acuerdo con la estructura del Instituto Nacional de Salud el mapa de procesos es el siguiente:



Fuente: http://www.ins.gov.co/Transparencia/estructura-organica-y-talento-humano/Paginas/procesos-y-procedimientos.aspx

ORGANIGRAMA:

De acuerdo con la estructura organizacional del Instituto Nacional de Salud el organigrama es el siguiente:



Fuente: https://www.mindomo.com/es/mindmap/organigrama-ins-aa65c3133847429397f87e10bf95f580

Con el sistema de gestión de seguridad de la información, la entidad conoce, los riesgos a los que está expuesta la información y los activos, y los asume, minimiza, transfiere o controla mediante una metodología definida, documentada y conocida por todos, que debe ser revisada y mejorada constantemente.

Que, en virtud de lo anterior, el INS requiere contratar la consultoría para realizar el diagnóstico del estado del MSPI, y continuar con las actividades necesarias para su implementación.

Definición técnica de la forma en que el Instituto puede satisfacer su necesidad

Mediante la contratación de una consultoría para realizar el diagnóstico del estado del modelo de seguridad y privacidad de la información (MSPI) del INS, la revisión y actualización de la documentación y el levantamiento de los riesgos en todos los procesos de la entidad para garantizar la confidencialidad, integridad y disponibilidad de la información generada en el Instituto Nacional durante el desarrollo de las actividades misionales.

Mencione la justificación del contrato en relación con el POA del área, citando la concordancia respectiva para el logro de los objetivos estratégicos:

- Objetivo Estratégico No. 1 Cumplir como institución pública de excelencia en el logro de sus objetivos y funciones misionales con calidad y oportunidad.
- Objetivo Específico No. 6 Ampliar la gestión interinstitucional, la presencia del INS en el territorio nacional y generar la integración de redes de su competencia.
- Actividad: 2.1.6.10.5.9. Continuar con la implementación del Modelo de Seguridad y Privacidad de la información (MSPI).

El presente proceso se encuentra incluido dentro del Plan Anual de Adquisiciones para la vigencia 2018 en la línea 24 OTIC.

Para realizar y cumplir con los lineamientos de los entes externos el INS se encuentra en la contratación por medio de un proceso de méritos y en la cual incluyo las siguientes fases:

Realizar las fases de análisis de brecha, establecimiento del Sistema de Gestión de Seguridad de la Información (SGSI), análisis de riesgos, pruebas de seguridad, plan estratégico de seguridad de la información, sensibilización y capacitación para la implementación del Modelo de Seguridad y Privacidad de la Información (MSPI) conforme a los lineamientos del Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC) y la Estrategia de Gobierno en Línea, contemplando la revisión, actualización de la documentación y el levantamiento de los riesgos de todos los procesos de la institución para garantizar la confidencialidad, integridad y disponibilidad de la información generada en el Instituto Nacional de Salud.

Las siguientes son las fases que se deberán desarrollar teniendo como referencia lo descrito en los lineamientos del documento *"Modelo de Seguridad y Privacidad de la Información (MSPI)"* del MinTIC alineados con el Marco de Referencia de Arquitectura Empresarial para la Gestión de TI (MRAE), la Estrategia de Gobierno en Línea (GEL) y la Norma Técnica Colombiana NTC-ISO-IEC 27001:2013 y demás documentación relacionada con el objeto del contrato:

FASE I: ANÁLISIS DE BRECHA		
ANÁLISIS GAP ISO 27001 y MSPI		
Objetivo	**Actividades**	**Productos**
Elaborar el análisis GAP (análisis de brecha) frente a la norma ISO 27000 y el Modelo de seguridad y privacidad de la información MSPI de INS.	• Conocer el negocio del INS, procesos definidos en el alcance, recursos que soportan los procesos, responsables del SGSI, tecnologías utilizadas y terceras partes involucradas. • Identificar y entender el contexto interno y externo del Instituto, partes interesadas y factores críticos de éxito. • Realizar entrevistas y recopilación de documentación con las personas responsables en los procesos de ejecutar las actividades contempladas en los controles, para identificar la forma como se ejecutan actualmente dichos controles.	• Informe de resultados del análisis, evaluación y diagnóstico de la situación actual e Identificación de brechas para cada dominio de ISO/IEC 27001:2013 y MSPI de Gobierno en Línea. • Recomendaciones sobre las brechas identificadas en el instrumento de evaluación y nivel de madurez en línea base de seguridad (MPSI).
	• Realizar un análisis GAP o de brecha al SGSI, siguiendo como marco de referencia la norma ISO 27001:2013, a fin de establecer el nivel de cumplimiento de la misma de acuerdo con el alcance definido por el INS y establecer el estado deseado del sistema.	
	• Estimar el nivel de cumplimiento de las normativas externas aplicables y políticas internas del INS.	
	• Elaborar el plan de recomendaciones para el cierre de las brechas identificadas y lograr un nivel de madurez aceptable para la Entidad.	• Plan de Acción para el cierre de las brechas detectadas.
	• Revisión de autorizaciones, avisos de privacidad, solicitudes, quejas y reclamos, procedimientos de gestión de incidentes y demás relacionados al cumplimiento de la ley de protección de datos	• Informe de diagnóstico de cumplimiento de ley 1581 de 2012 y responsabilidad demostrada.

FASE I: ANÁLISIS DE BRECHA		
ANÁLISIS GAP ISO 27001 y MSPI		
Objetivo	**Actividades**	**Productos**
	personales desde la perspectiva de responsabilidad demostrada (se deben tener en cuenta la existencia de otras leyes o normativas que tengan relación como la Ley de transparencia).	
	• Realizar el diligenciamiento del instrumento de evaluación, identificación y nivel de madurez en línea base de seguridad (MSPI), de acuerdo con lo establecido en GEL.	• Instrumento de evaluación diligenciado, identificación y nivel de madurez en línea base de seguridad (MSPI), de acuerdo con lo establecido en GEL.

FASE II: ESTABLECIMIENTO DEL SGSI		
DISEÑO DE POLITICAS Y PROCEDIMIENTOS DE SEGURIDAD		
Objetivo	**Actividades**	**Productos**
Diseñar políticas y procedimientos de seguridad conforme la estructura propuesta por la norma ISO 27000 alineados al Sistema Integrado de Gestión de la Entidad.	Construir el manual de políticas y procedimientos respetando la estructura propuesta por la norma ISO 27000, de acuerdo con: • Resultados del análisis GAP. • Requerimientos y normativas que deba satisfacer la organización • Las buenas prácticas de seguridad,	• Documento de la definición de los objetivos del SGSI • Documento de la definición del alcance del SGSI. • Documento del procedimiento actual de Revisión por la Dirección del Sistema Integrado de Gestión de Calidad - SIGC frente a los requisitos del SGSI.
	Como mínimo se deberá elaborar o actualizar las políticas y procedimientos alineado a lo exigido por la norma ISO 27001:2013 y por MPSI. **Políticas**: 1. BYOD 2. Capacitación y Sensibilización en Seguridad de Información 3. Clasificación de la información 4. Confidencialidad 5. Contraseñas 6. Control de acceso	• Definición Indicadores de Gestión. • Entrega como mínimo de las 24 políticas y 25 procedimientos anteriormente enunciados de seguridad de la información, considerados en los 14 dominios de la norma ISO 27001:2013 y el MSPI.

FASE II: ESTABLECIMIENTO DEL SGSI		
DISEÑO DE POLITICAS Y PROCEDIMIENTOS DE SEGURIDAD		
Objetivo	**Actividades**	**Productos**
	7. Controles criptográficos 8. Copias de seguridad 9. Disponibilidad 10. Dispositivo sobre dispositivos móviles y teletrabajo 11. Eliminación y destrucción 12. Ética empresarial 13. Gestión de Activos 14. Gestión de cambios 15. Gestión de Incidentes de Seguridad de Información y Datos Personales 16. Integridad 17. No repudio 18. Pantalla y escritorio limpios 19. Registro y Auditoria 20. Seguridad de la información y objetivos 21. Seguridad para proveedores 22. Transferencia de información 23. Tratamiento de Datos Personales 24. Uso aceptable **Procedimientos:** 1. Adquisición, desarrollo y mantenimiento de sistemas de información 2. Aseguramiento de servicios en la red 3. Capacitación y sensibilización del personal 4. Control de acceso físico 5. Control de software 6. Control para código malicioso 7. Controles criptográficos	
	8. Gestión de cambios 9. Gestión de capacidad 10. Gestión de llaves criptográficas 11. Gestión de usuarios y contraseñas 12. Identificación y clasificación de activos 13. Ingreso y desvinculación del personal 14. Mantenimiento de equipos 15. Protección de activos 16. Retiro de activos 17. Separación de ambientes 18. Transferencia de información	

FASE II: ESTABLECIMIENTO DEL SGSI		
DISEÑO DE POLITICAS Y PROCEDIMIENTOS DE SEGURIDAD		
Objetivo	**Actividades**	**Productos**
	19. Acciones correctivas 20. Auditoría interna 21. Gestión de incidentes 22. Ingreso seguro a los sistemas de información 23. Continuidad de negocio 24. Operación para gestión de ti 25. Trabajo en áreas seguras	

FASE II: ESTABLECIMIENTO DEL SGSI		
DEFINICION DE LA ESTRUCTURA ORGANIZACIONAL SEGURIDAD DE LA INFORMACION		
Objetivo	**Actividades**	**Productos**
Emitir una propuesta con las recomendaciones sobre la estructura y ubicación en el organigrama institucional de la función de seguridad de la información ajustada al contexto interno del INS y teniendo en cuenta sus necesidades.	Proponer el perfil y competencias necesarias del personal a cargo del SGSI y capacitación necesaria para el mantenimiento de la organización de la seguridad de la información. Realizar reuniones con la alta dirección y definir una propuesta sobre la estructura organizacional, incluyendo los roles y responsabilidades de los interesados. Proponer las funciones y responsabilidades de los perfiles a continuación: • Oficial de seguridad. • Analista de monitoreo e incidentes.	Documento propuesto de la estructura organizacional de SI con las competencias técnicas y organizacionales que debe tener cada uno de los integrantes en la organización de la seguridad, Propuesta del plan de entrenamiento para lograr las competencias requeridas para el mantenimiento del sistema de gestión de seguridad de la información. Propuesta de Organigrama del SGSI y MPSI. Propuesta de Roles y responsabilidades del SGSI y MPSI
	• Analista SGSI. • Analista de tecnología de seguridad. • Administración de accesos. • Ingeniero de redes. Proponer las funciones y responsabilidades de los comités Proponer los perfiles y formación requeridos por los diferentes roles, teniendo en cuenta aspectos como:	

FASE II: ESTABLECIMIENTO DEL SGSI		
DEFINICION DE LA ESTRUCTURA ORGANIZACIONAL SEGURIDAD DE LA INFORMACION		
Objetivo	**Actividades**	**Productos**
	• Formación • Experiencia • Certificaciones • Conocimientos en seguridad • Conocimientos y capacidades generales Propuesta de conformación de comités, como mínimo: • Comité de seguridad • Comité de gestión de incidentes	
	• Analista SGSI. • Analista de tecnología de seguridad. • Administración de accesos. • Ingeniero de redes. Proponer las funciones y responsabilidades de los comités Proponer los perfiles y formación requeridos por los diferentes roles, teniendo en cuenta aspectos como: • Formación • Experiencia • Certificaciones • Conocimientos en seguridad • Conocimientos y capacidades generales Propuesta de conformación de comités, como mínimo: • Comité de seguridad • Comité de gestión de incidentes	

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)	Identificar cuáles son las métricas e indicadores adecuadas que resulten	• Definición de indicadores de

FASE II: ESTABLECIMIENTO DEL SGSI		
DEFINICION E IMPLEMENTACIÓN DEL MODELO DE MEDICIÓN DEL SGSI		
Objetivo	**Actividades**	**Productos**
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	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.	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**:	• Inventario de activos de información. • Inventario de bases de datos personales.

FASE III: ANÁLISIS DE RIESGOS		
IDENTIFICACIÓN DE ACTIVOS DE INFORMACIÓN		
Objetivo	**Actividades**	**Productos**
	• Procesos y actividades del negocio • Información (Datos e Información Impresa)	
	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 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	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.

FASE IV: PRUEBAS DE SEGURIDAD		
HACKING ÉTICO Y PENETRACIÓN		
Objetivo	**Actividades**	**Productos**
	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 • KALI Pentest FrameWork • Web Application Attack and Audit FrameWork • Tenable Nessus Professional Feed • Nmap	Recomendaciones sobre aspectos a mejorar a nivel de cultura de seguridad.

FASE IV: PRUEBAS DE SEGURIDAD		
INGENIERÍA SOCIAL		
Objetivo	**Actividades**	**Productos**
Mediante estas pruebas se busca evidenciar las vulnerabilidades que existen dentro del INS, buscando obtener información de personas y procesos claves del negocio mediante acceso físico a la misma o con información de acceso facilitada por el personal de la organización, el cual ha sido objeto de engaño.	**INGENIERÍA SOCIAL:** Presentación de la metodología a utilizar. Determinar entre las partes el perfil de los funcionarios a los cuales se les debe realizar pruebas de ingeniería social (20) Elaboración de los instrumentos y herramientas a utilizar de acuerdo con el perfil de los empleados a evaluar y las pruebas aprobadas	Documento de Ingeniería Social que contenga la descripción de la información conseguida, la forma de conseguirla, la fecha y las personas con las que se consiguió según el alcance para veinte (20) funcionarios de la entidad. Descripción de los problemas encontrados, la forma en que se pueden aprovechar y las recomendaciones para corregir y minimizar los riesgos detectados.
	Realización de las pruebas de ingeniería social, como mínimo: ○ Pruebas con correos electrónicos tipo Phishing (mínimo 20 correos). ○ Pruebas con llamadas	Documento con las recomendaciones en base a los resultados obtenidos en las pruebas y su socialización.

FASE IV: PRUEBAS DE SEGURIDAD		
INGENIERÍA SOCIAL		
Objetivo	**Actividades**	**Productos**
	telefónicas (mínimo 20 llamadas).	
FASE V: PLAN ESTRATEGICO DE SEGURIDAD DE LA INFORMACIÓN - PESI		
Objetivo	**Actividades**	**Productos**
Identificar el conjunto de responsabilidades, prácticas y acciones a ser desarrolladas por la organización con miras a propender que los riesgos de la información sean apropiadamente administrados, mediante la definición de un modelo de seguridad de la información, alineado con las mejores prácticas, estándares y objetivos del negocio.	En base al conocimiento de la organización y resultados del diagnóstico de la seguridad de la información y documentación resultante de estas actividades en la etapa de diagnóstico, como también de los resultados obtenidos en el análisis de riesgos y pruebas de seguridad se deberán realizar las actividades complementarias que sirvan de insumo para la elaboración del PESI, como son: • Alinear los Objetivos de la seguridad de la información con los objetivos del negocio.	Plan Estratégico de Seguridad de la Información PESI a tres (3) años.
	• Identificar el portafolio de proyectos e iniciativas a priorizar en el PESI con los recursos humanos y financieros aproximados • Elaborar una matriz con la estimación aproximada de recursos, tiempos de referencia para su implementación, justificación y priorización	

FASE VI: SENSIBILIZACIÓN Y ENTRENAMIENTO EN SEGURIDAD DE LA INFORMACIÓN		
CHARLAS DE SENSIBILIZACIÓN		
Objetivo	**Actividades**	**Productos**
Entender el estado actual de la organización en cuanto a cultura de seguridad de la información para emitir las recomendaciones y acciones necesarias para elevar la misma	• Establecer las acciones necesarias para dimensionar e implementar el programa de concienciación y entrenamiento requerido por la organización en lo referente a seguridad de la información tomando como insumo los resultados de las pruebas de ingeniería social. • • Identificar el estado actual de la conciencia en seguridad de la	Informe de divulgación el cual contiene: • Diseño de Plan de Sensibilización • Informe de actividades de sensibilización (4 charlas para aproximadamente 400 asistentes). • 70 recordatorios de sensibilización en seguridad de la información Entrega del material empleado en las charlas para futuras capacitaciones (video de las charlas, presentaciones,

FASE VI: SENSIBILIZACIÓN Y ENTRENAMIENTO EN SEGURIDAD DE LA INFORMACIÓN		
CHARLAS DE SENSIBILIZACIÓN		
Objetivo	**Actividades**	**Productos**
	información mediante un plan de entrevistas a funcionarios claves del INS. • • Identificar los planes necesarios de concientización/capacitación en seguridad de la información determinando los grupos objetivos, material requerido e identificación de los objetivos de comunicación y divulgación.	pendones, afiches, diseños gráficos, entre otros). Resultados de la evaluación sobre los temas de las charlas de seguridad de la información. Planillas de registro de asistencia de los funcionarios a las charlas. .
	• Realizar una evaluación que permita medir el conocimiento asimilado por los funcionarios capacitados en temas de seguridad informática. • Elaborar un informe con los resultados del proceso y dar las recomendaciones de la importancia de implementar estrategias de concientización y capacitación. • Socializar el informe del proceso de concientización y capacitación.	

FASE VI: SENSIBILIZACIÓN Y ENTRENAMIENTO EN SEGURIDAD DE LA INFORMACIÓN		
AUDITORIA INTERNA SGSI		
Objetivo	**Actividades**	**Productos**
Desarrollar actividades preparatorias que busquen orientar a la organización para afrontar el proceso de auditoría por parte de un ente certificador el cual comprenderá efectuar una revisión y cumplimiento del SGSI frente a los requerimientos exigidos para la certificación ISO 27001:2013. **Alcance:** La auditoría se ejecutará	• Proveer el grado de preparación que tiene la organización para afrontar una auditoría de tercera parte con miras a la certificación del SGSI. • Realizar la recolección de evidencia suficiente y probatoria sobre el cumplimiento de los requisitos que exige la norma ISO 27001:2013 para la certificación del SGSI.	• Plan de auditoría aprobado entre las partes. • Informe de Auditoría de cumplimiento del SGSI • Plan de Acción para el cierre de No conformidades. • Recomendaciones para afrontar una auditoria de certificación del SGSI por tercera parte. • Capacitación en: ISO 27001:2013 Auditor interno para nueve (9)

FASE VI: SENSIBILIZACIÓN Y ENTRENAMIENTO EN SEGURIDAD DE LA INFORMACIÓN		
AUDITORIA INTERNA SGSI		
Objetivo	**Actividades**	**Productos**
siguiendo los lineamientos de los entes certificadores en un tiempo máximo de 5 días.		funcionarios de INS. • Certificado de asistencia al curso para los funcionarios que cumplan con la intensidad horaria mínima requerida.

POLITICAS Y PROCEDIMIENTOS

En las tablas 1 y 2 a continuación se especifican las políticas y procedimientos del INS a revisar y actualizar, los cuales deberán estar alineados a lo exigido por la norma ISO 27001:2013, al MPSI y al Sistema Integrado de Gestión de la Entidad. En caso de no existir dichas políticas o procedimientos estos deberán ser elaborados:

TABLA 1 – PROCEDIMIENTOS

Item	Descripción procedimientos	ISO 27001:2013	MSPI
1	Procedimiento de adquisición, desarrollo y mantenimiento de sistemas de información		X
2	Procedimiento de aseguramiento de servicios en la red		X
3	Procedimiento de Capacitación y Sensibilización del Personal		X
4	Procedimiento de control de acceso físico		X
5	Procedimiento de Control de Software		X
6	Procedimiento de control para código malicioso		X
7	Procedimiento de Controles Criptográficos		X
8	Procedimiento de Gestión de Cambios		X
9	Procedimiento de Gestión de Capacidad		X
10	Procedimiento de Gestión de Llaves Criptográficas		X
11	Procedimiento de gestión de usuarios y contraseñas		X
12	Procedimiento de identificación y Clasificación de activos		X
13	Procedimiento de Ingreso y Desvinculación del Personal		X
14	Procedimiento de Mantenimiento de Equipos		X
15	Procedimiento de protección de activos		X
16	Procedimiento de retiro de activos		X
17	Procedimiento de separación de Ambientes		X
18	Procedimiento de transferencia de información		X
19	Procedimiento para acciones correctivas	X	

Item	Descripción procedimientos	ISO 27001:2013	MSPI
20	Procedimiento para auditoría interna	X	
21	Procedimiento para control de documentos	X	
22	Procedimiento para el tratamiento de la seguridad en los acuerdos con los proveedores		X
23	Procedimiento para gestión de incidentes	X	X
24	Procedimiento para ingreso seguro a los sistemas de información		X
25	Procedimientos de continuidad de negocio	X	X
26	Procedimientos de operación para gestión de TI	X	
27	Procedimientos para trabajo en áreas seguras	X	

TABLA 2 – POLITICAS

Ítem	Descripción políticas	ISO 27001:2013	MSPI
1	Política BYOD	X	
2	Política de Capacitación y Sensibilización en Seguridad de Información		
3	Política de clasificación de la información	X	X
4	Política de Confidencialidad		X
5	Política de contraseñas	X	
6	Política de control de acceso	X	X
7	Política de Controles Criptográficos		X
8	Política de Copias de seguridad	X	
9	Política de Disponibilidad		X
10	Política de dispositivo sobre dispositivos móviles y teletrabajo	X	
11	Política de eliminación y destrucción	X	
12	Política de Ética Empresarial		X
13	Política de Gestión de Activos		X
14	Política de gestión de cambios	X	
15	Política de Gestión de Incidentes de Seguridad de Información y Datos Personales		X
16	Política de Integridad		X
17	Política de No Repudio		X
18	Política de pantalla y escritorio limpios	X	X
19	Política de Registro y Auditoria		X
20	Política de seguridad de la información y objetivos	X	X
21	Política de seguridad para proveedores	X	
22	Política de transferencia de información	X	
23	Política de Tratamiento de Datos Personales		X

Ítem	Descripción políticas	ISO 27001:2013	MSPI
24	Política de Uso Aceptable		X

a) verificando la seguridad de la información durante su realización y la documentación de dichas pruebas.

CRONOGRAMA

CRONOGRAMA PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Nombre Tarea		2018						
	May	Jun	Jul	Ago	Sep	Oct	Nov	Dic
Radicación de estudios ´previos								
CONTEXTO DE LA ORGANIZACIÓN								
Comprensión De Las Necesidades Y Expectativas De Las Partes Interesadas								
Determinación del alcance del sistema de gestión de la seguridad de la información								
LIDERAZGO								
Política de Seguridad de la Información								
Roles, Responsabilidades y Autoridades de Seguridad de la Información								
Política de Segregación de Funciones								
Apoyo e la identificación de contenido de seguridad y protección de la información en Acuerdo de Confidencialidad y Transparencia								
SOPORTE								
Toma de conciencia								
Documentación de Sistema de Gestión de Seguridad de la Información (manuales, políticas, procedimientos, instructivos, formatos, etc								
EVALUACION DE DESEMPEÑO								
Seguimiento, Medición y Evaluación de seguridad de la información								
Auditoría Interna de seguridad de la Información								
Revisión por la Dirección								
CONTROLES DE SEGURIDAD DE LA INFORMACION								
Contacto con Autoridades y grupos de interes								
Propuesta seguridad de la información en proyectos								
Inventario de Activos de Información (proceso tecnológico, evaluación de propuestas - sala, Gestión Documental								
Inventario Procesos tecnológico								
Inventario Proceso evaluación de propuestas - Sala de Evaluación								

Inventario Archivo y Gestión documental								
Inventario Seguridad Física y ambiental								
Talento Humano								
Lineamientos de uso aceptable de Activos de Información								
CROGRAMA PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN								
Nombre Tarea		**2018**						
	May	**Jun**	**Jul**	**Ago**	**Sep**	**Oct**	**Nov**	**Dic**
SEGURIDAD FISICA								
Valoración de la seguridad física y de entorno de las áreas seguras (Centro de datos ANI y de cableados en pisos)								
Apoyo en el protocolo de seguridad de la sala de evaluación de propuestas								
SEGURIDAD DE LAS COMUNICACIONES								
Definición de políticas de acceso seguro y uso adecuado del servicio de internet								
Política de configuración y aseguramiento de conexión inalámbrica								
INCIDENTES DE SEGURIDAD DE LA INFORMACION								
Establecimiento del modelo de gestión de incidentes de seguridad de la información								
CONTINUIDAD DE NEGOCIO								
Ejecución de actividades para el establecimiento del BIA (Business Impact Analysis de la ANI)								
CUMPLIMIENTO								
Apoyo en la identificación de la legislación aplicable a seguridad y protección de la información (normograma)								

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