# PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Instituto Nacional de Vigilancia de Medicamentos y Alimentos - Invima
**Bogotá**
Principal: Cra 10 N° 64 - 28
Administrativo: Cra 10 N° 64 - 60
(1) 2948700
**www.invima.gov.co**

GP-202-1
SC7341-1
CO-SC73-41-1

CONTENIDO

1. Objetivo ..... 3
2. Alcance ..... 3
3. Plan de tratamiento de riesgos de seguridad y privacidad de la información ..... 3
3.1. Planes desarrollados de riesgos de seguridad y privacidad de la información ..... 3
3.2. Riesgos de seguridad y privacidad de la información ..... 3
3.3. Actividades para desarrollar sobre los riesgos de seguridad y privacidad de la información ..... 5
3.4. Programación de monitoreo de controles de riesgos de seguridad y privacidad de la información ..... 6
4. Marco legal ..... 6
5. Requisitos técnicos ..... 7
6. Responsable del documento ..... 7

## 1. Objetivo

Definir los controles con los cuales se buscan mitigar la materialización de los riesgos de seguridad de la información en el Instituto Nacional de Vigilancia de Medicamentos y Alimentos INVIMA. Así como el tratamiento de los riesgos de la Seguridad y Privacidad de la Información.

## 2. Alcance

El plan de tratamiento de riesgos tiene alcance para los procesos del Instituto Nacional de Vigilancia de Medicamentos y Alimentos INVIMA, en concordancia con el alcance del Sistema de Gestión de Seguridad de la Información.

## 3. Plan de tratamiento de riesgos de seguridad y privacidad de la información

Con el fin de prevenir la materialización de las amenazas que pueden afectar la disponibilidad confidencialidad o integridad de la información del Instituto Nacional de Vigilancia de Medicamentos y Alimentos INVIMA, se presenta a continuación los planes definidos para la identificación de los riesgos y su seguimiento.

### 3.1. Planes desarrollados de riesgos de seguridad y privacidad de la información

Durante la vigencia 2018 se definieron y desarrollaron las actividades necesarias para la identificación de los riesgos de seguridad de la información su inclusión en el sistema de gestión integrado. Estas actividades fueron:

- Revisión del Formato SGI-EMC-FM001 Acciones de mejora
- Declaración de aplicabilidad
- Identificación de riesgos de seguridad de la información para los activos más importantes de los procesos GTH - Gestión de Talento Humano, GPR - Gestión del Presupuesto, GCO - Gestión Contable, ABS - Adquisición de Bienes y Servicios, GDO - Gestión Documental y Correspondencia, GJE - Gestión de Procesos Judiciales y Extrajudiciales, GIN - Gestión Informática y de la Información, GIN - Gestión Informática y de la Información.
- Revisión de la Matriz consolidada de riesgos del INVIMA
- Actualización de riesgos identificados como operativos a riesgos de seguridad de la Información
- Diligenciamiento de los riesgos de seguridad en el formato SGI-EMC-FM006 Identificación de Riesgos INVIMA
- Socialización con planeación de los riesgos de seguridad identificados

### 3.2. Riesgos de seguridad y privacidad de la información

Dentro de los ejercicios realizados en el 2018 la oficial de seguridad de la información junto con la oficina de planeación establece que durante la vigencia del presente año (2019) se modificará la guía de riesgos del

INVIMA, con el fin de incluir los riesgos de seguridad de la información de acuerdo con los lineamientos dados por el DAFP en su guía de gestión de riesgos versión número 4 de octubre del 2018.

A continuación, se presentan los riesgos identificados el año inmediatamente anterior:

| Nombre | Estado del riesgo | Proceso responsable | Materializado |
|---|---|---|---|
| Pérdida de integridad en la información diligenciada en la Nómina y sus novedades dentro del aplicativo de Nomina | Por socializar | GTH - Gestión de Talento Humano | No |
| Pérdida de integridad en el registro de la ejecución presupuestal | Por socializar | GPR - Gestión del Presupuesto | No |
| Pérdida de Integridad en las causaciones de retención a las obligaciones financieras de la entidad. | Por socializar | GCO - Gestión Contable | No |
| Indisponibilidad de la información por pérdida de expedientes físicos contractuales y/o documentación relacionada. | Por socializar | ABS - Adquisición de Bienes y Servicios | No |
| Pérdida de disponibilidad parcial o total de la información del archivo de gestión y central | Por socializar | GDO - Gestión Documental y Correspondencia | No |
| Pérdida de integridad por adulterar, sustraer, copiar eliminar de manera parcial o total información del archivo de gestión y central. | Por socializar | GDO - Gestión Documental y Correspondencia | No |
| Perdida de confidencialidad por acceso no autorizado que permita adulterar, sustraer, eliminar o divulgar de manera parcial o total información del archivo de gestión y central. | Por socializar | GDO - Gestión Documental y Correspondencia | No |
| Pérdida de integridad de la documentación física por deficiente aplicación del protocolo de limpieza documental. | Por socializar | GDO - Gestión Documental y Correspondencia | No |
| Pérdida de la integridad de la información del estado y cantidad de los procesos judiciales en el Invima administrados mediante la base de datos de procesos judiciales. | Por socializar | GJE - Gestión de Procesos Judiciales y Extrajudiciales | No |
| Pérdida de confidencialidad de la información almacenada en las bases de datos administradas por la Oficina de tecnologías de la información. | Por socializar | GIN - Gestión Informática y de la Información | No |
| Pérdida de integridad de la información por incorrecto procesamiento de los datos debido a versiones de software desactualizadas luego de entregar las soluciones desarrolladas. | Por socializar | GIN - Gestión Informática y de la Información | No |

## 3.3. Actividades para desarrollar sobre los riesgos de seguridad y privacidad de la información

| Actividad | Responsable | Fecha inicial planificada | Fecha final planificada |
|---|---|---|---|
| Implementación de los lineamientos del SGSI, formación y sensibilización | Oficial de Seguridad de la Información<br>Personal que hace parte del proceso | Mayo de 2019 | Noviembre de 2019 |
| Implementación de los lineamientos del SGSI, socialización de los procesos y procedimientos, formación y sensibilización | Oficial de Seguridad de la Información<br>Personal que hace parte del proceso<br>Responsables de Calidad | Mayo de 2019 | Noviembre de 2019 |
| Implementación de los lineamientos del SGSI, formación y sensibilización | Oficial de Seguridad de la Información<br>Personal que hace parte del proceso | Mayo de 2019 | Noviembre de 2019 |
| Implementación de los lineamientos del SGSI, socialización de los procesos y procedimientos, formación y sensibilización | Oficial de Seguridad de la Información<br>Personal que hace parte del proceso<br>Responsables de Calidad | Mayo de 2019 | Noviembre de 2019 |
| Implementación de los lineamientos del SGSI, socialización de los procesos y procedimientos, formación y sensibilización | Oficial de Seguridad de la Información<br>Personal que hace parte del proceso<br>Responsables de Calidad | Mayo de 2019 | Noviembre de 2019 |
| Implementación de los lineamientos del SGSI, socialización de los procesos y procedimientos, formación y sensibilización | Oficial de Seguridad de la Información<br>Personal que hace parte del proceso<br>Responsables de Calidad | Mayo de 2019 | Noviembre de 2019 |
| Implementación de los lineamientos del SGSI, socialización de los procesos y procedimientos, formación y sensibilización | Oficial de Seguridad de la Información<br>Personal que hace parte del proceso<br>Responsables de Calidad | Mayo de 2019 | Noviembre de 2019 |
| Implementación de los lineamientos del SGSI, socialización de los procesos y procedimientos, formación y sensibilización | Oficial de Seguridad de la Información<br>Personal que hace parte del proceso<br>Responsables de Calidad | Mayo de 2019 | Noviembre de 2019 |

| Actividad | Responsable | Fecha inicial planificada | Fecha final planificada |
|---|---|---|---|
| Identificación de la información sensible<br>Definición de mecanismos de control y protección | Oficial de Seguridad de la Información<br>Personal que hace parte del proceso<br>Responsables de Calidad | Mayo de 2019 | Noviembre de 2019 |
| La dependencia responsable de la información deberá validar el tipo de información solicitada por los usuarios para determinar su entrega conforme a la Ley 1712 del 06 de marzo de 2014, título IV, capítulos I y II que tratan sobre Información pública clasificada e Información pública<br>reservada respectivamente. | Responsable del proceso | Mayo de 2019 | Noviembre de 2019 |
| Identificación de los activos de información su sensibilidad<br>Correcta aplicación de los procedimientos definidos<br>Implementación de los lineamientos del SGSI | Responsable del proceso<br>Personal que hace parte del proceso<br>Responsables de Calidad<br>Oficial de Seguridad de la Información | Mayo de 2019 | Noviembre de 2019 |

### 3.4. Programación de monitoreo de controles de riesgos de seguridad y privacidad de la información

La programación del seguimiento se hará en cualquiera de las siguientes situaciones:

- Semestralmente
- Si se presenta un cambio en el proceso implicado.
- Se materializa una amenaza.

## 4. Marco legal

- Constitución Política de Colombia 1991. Artículo 15. Reconoce como Derecho Fundamental el Habeas Data y Artículo 20. Libertad de Información.
- Decreto 612 de 4 de abril de 2018, Por el cual se fijan directrices para la integración de los planes institucionales y estratégicos al Plan de Acción por parte de las Entidades del Estado.
- Decreto 1008 de 14 de junio de 2018, Por el cual se establecen los lineamientos generales de la política de Gobierno Digital.

## 5. Requisitos técnicos

- Norma Técnica Colombiana NTC/ISO 27001:2013 Sistemas de gestión de la seguridad de la información.
- Modelo de Seguridad y Privacidad de la Información, Ministerio de Tecnologías y Sistemas de Información.
- Decreto 612 de 2018: Por el cual se fijan directrices para la integración de los planes institucionales y estratégicos al Plan de Acción por parte de las entidades del Estado, entre los que menciona el plan de tratamiento de riesgos de seguridad de la información.

## 6. Responsable del documento

Oficial de Seguridad de la Información y Dirección General