1. OBJETIVO

Establecer e implementar metodologías para minimizar y mantener los riesgos de seguridad de la información en un nivel aceptable para la Agencia, mejorando continuamente la eficacia en la gestión de seguridad.

2. ALCANCE

Cubre el centro de información y cada una de las dependencias de la Agencia iniciando con el análisis y terminando con la gestión de vulnerabilidades.

3. RESPONSABLE

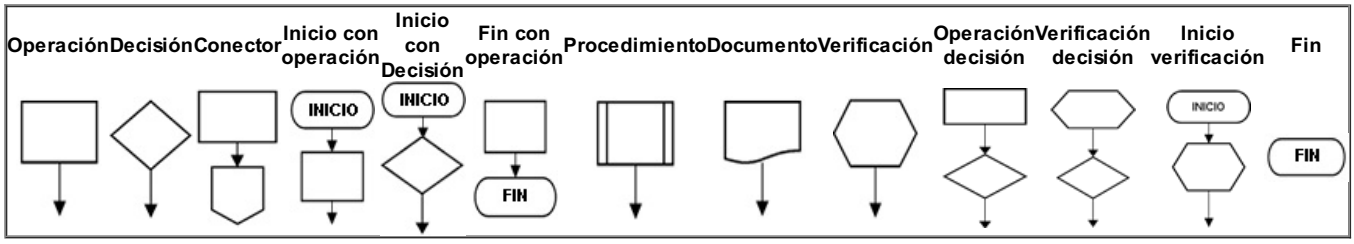
Subdirección Administrativa, Financiera y de Apoyo a la Gestión y Área de Sistemas de Información.

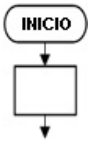
4. DEFINICIONES

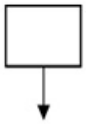
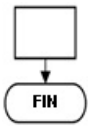
- **Antispam:** El antispam es lo que se conoce como método para prevenir el "correo basura". Tanto los usuarios finales como los proveedores de servicios de correo electrónico utilizan diversas técnicas contra ello. Algunas de estas técnicas han sido incorporadas en productos, servicios y software para aliviar la carga que cae sobre usuarios y administradores
- **Firewall:** Un cortafuego (firewall), es un sistema o dispositivo que permite proteger a una computadora o una red de computadoras de las intrusiones que provienen de una tercera red (expresamente de Internet).
- **Filtrado web:** Un filtro web, denominado normalmente "software de control de contenidos", es un tipo de software diseñado para restringir los sitios web que puede visitar un usuario en su ordenador. Estos filtros pueden utilizar una lista blanca o una lista negra: la lista blanca solo ofrece acceso a sitios seleccionados específicamente por la persona que configuró el filtro y la lista negra restringe el acceso a sitios no deseados determinados por los estándares instalados en el filtro.
- **Seguridad informática:** Disciplina que se encarga de proteger la integridad y la privacidad de la información almacenada en un sistema informático
- **Virus informático:** Los virus son programas informáticos que tienen como objetivo alterar el funcionamiento del computador, sin que el usuario se dé cuenta. Estos, por lo general, infectan otros archivos del sistema con la intensión de modificarlos para destruir de manera intencionada archivos o datos almacenados en tu computador.
- **Vulnerabilidad informática:** Debilidad del sistema informático que puede ser utilizada para causar un daño. Las debilidades pueden aparecer en cualquiera de los elementos de una computadora, tanto en el hardware, el sistema operativo, cómo en el software.

5. CONDICIONES INICIALES

6. DESCRIPCIÓN DE ACTIVIDADES



N°	Actividad	Flujograma	Cargo Responsable	Referencia
1	**Identificar riesgos de seguridad:** Se analizan las actividades reportadas en formato F-AP-SI-008 Consolidado de Soporte Técnico en busca de posibles riesgos a nivel de seguridad reportados por los usuarios. Si se encuentran riesgos de seguridad se tipifica en las categorías; seguridad informática, alertas en la plataforma de antivirus y anomalías detectadas en los servidores de la Agencia, con el fin de establecer su gestión y posible solución. Este proceso se documenta en el formato F-AP-SI-012 Identificación de riesgo de seguridad.		Técnico o Profesional de Sistemas	F-AP-SI-012 Identificación de riesgo de seguridad

	Nota: Algunos procesos de seguridad son innatos a los equipos de infraestructura de la agencia, como lo son el firewall, el filtrado web y la seguridad de servidores, que se realizan de manera automática o con cierta periodicidad. Previa configuración de los equipos por parte personal técnico.			
2	**Implementar soluciones:** - Se investiga la vulnerabilidad detectada y se procede a implementar la posible solución. - Se analiza el reporte de plataforma de antivirus y se actualizan firmas de antivirus. - Se aplican las restricciones de firewall, filtrado web y bloqueos antispam (si existen).		Técnico o Profesional de Sistemas	F-AP-SI-012 Identificación de riesgo de seguridad
3	**Realizar seguimiento de vulnerabilidades:** Dependiendo del tipo de vulnerabilidad detectada se realiza un seguimiento (se registra en el formato F-AP-SI-005 Identificación de riesgo de seguridad – fecha revisión) o se da por solucionado el riesgo.		Técnico o Profesional de Sistemas	F-AP-SI-012 Identificación de riesgo de seguridad.

7. DOCUMENTOS DE REFERENCIA

- Seguridad informática
- Vulnerabilidad informática
- Virus informático
- Firewall
- Filtrado web
- Antispam

8. LISTADO DE ANEXOS

- F-AP-SI-012 Identificación de riesgo de seguridad

9. HISTORIAL DE CAMBIOS

VERSIÓN	FECHA	RAZÓN DE LA ACTUALIZACIÓN
1	10/May/2018	

ELABORÓ	REVISÓ	APROBÓ
Nombre: Juan Pablo Hernández Grisales **Cargo:** Contratista Lider Gestión de Sistemas de Información **Fecha:** 10/May/2018	**Nombre:** José Alveiro Giraldo Gómez **Cargo:** Subdirector Administrativo, Financiero y de Apoyo a la Gestión **Fecha:** 10/May/2018	**Nombre:** Sistema Integrado de Gestión **Cargo:** Profesional 1 **Fecha:** 10/May/2018