1. OBJETIVO

Establecer el flujo de actividades para las solicitudes de publicación de aplicaciones hacia internet, permitiendo la revisión, aprobación y configuración los controles de seguridad para su protección.

2. ALCANCE

En este procedimiento define el flujo de actividades desde los formatos para su solicitud y aprobación, hasta las actividades de configuración de controles de seguridad.

3. NORMATIVIDAD

Ver Normograma.

4. DEFINICIONES

• **Aplicación:** Es un tipo de programa Informático diseñado para facilitar al usuario la realización de un determinado tipo de trabajo.

• **APP**: Aplicación WEB.

• **Procedimiento**: Son utilizados para delinear los pasos que deben ser seguidos por una dependencia para implementar algo, para el propósito de este documento es la seguridad relacionada a dicho proceso o sistema específico. Generalmente los procedimientos son desarrollados, implementados y supervisados por el encargado del proceso o del sistema.

• **Seguridad de la información**: Preservación de la confidencialidad, integridad y disponibilidad de la información.

• **Servidor:** un computador que ofrece servicios a máquinas de cliente distantes o a aplicaciones, como el suministro de contenidos de páginas u otros recursos.

• **WAF (Web Application Firewall):** Cortafuegos para aplicaciones Web en internet.

5. POLÍTICAS DE OPERACIÓN

A continuación, se especifican las políticas de operación para la solicitud de publicación de APP a internet.

- ✓ Para la aprobación de publicación de una aplicación hacia internet, deberá estar revisada y aprobada por el jefe inmediato y el jefe de la oficina de informática.

- ✓ Para la formalización y aprobación de la solicitud de publicación es necesario diligenciar los siguientes (2) dos formatos E-GI-F036 FORMATO PUBLICACIÓN DE APP EN INTERNET y E-GI-F006 FORMATO SOLICITUD CAMBIO O ADICION COPIAS RESPALDO, que se encuentran en el Sistema de Gestión Integrado – SGI en el grupo de Gestión de tecnología de Información y Comunicaciones.

- ✓ Las aplicaciones que se van a publicar hacia internet deberán estar en un servidor de producción.

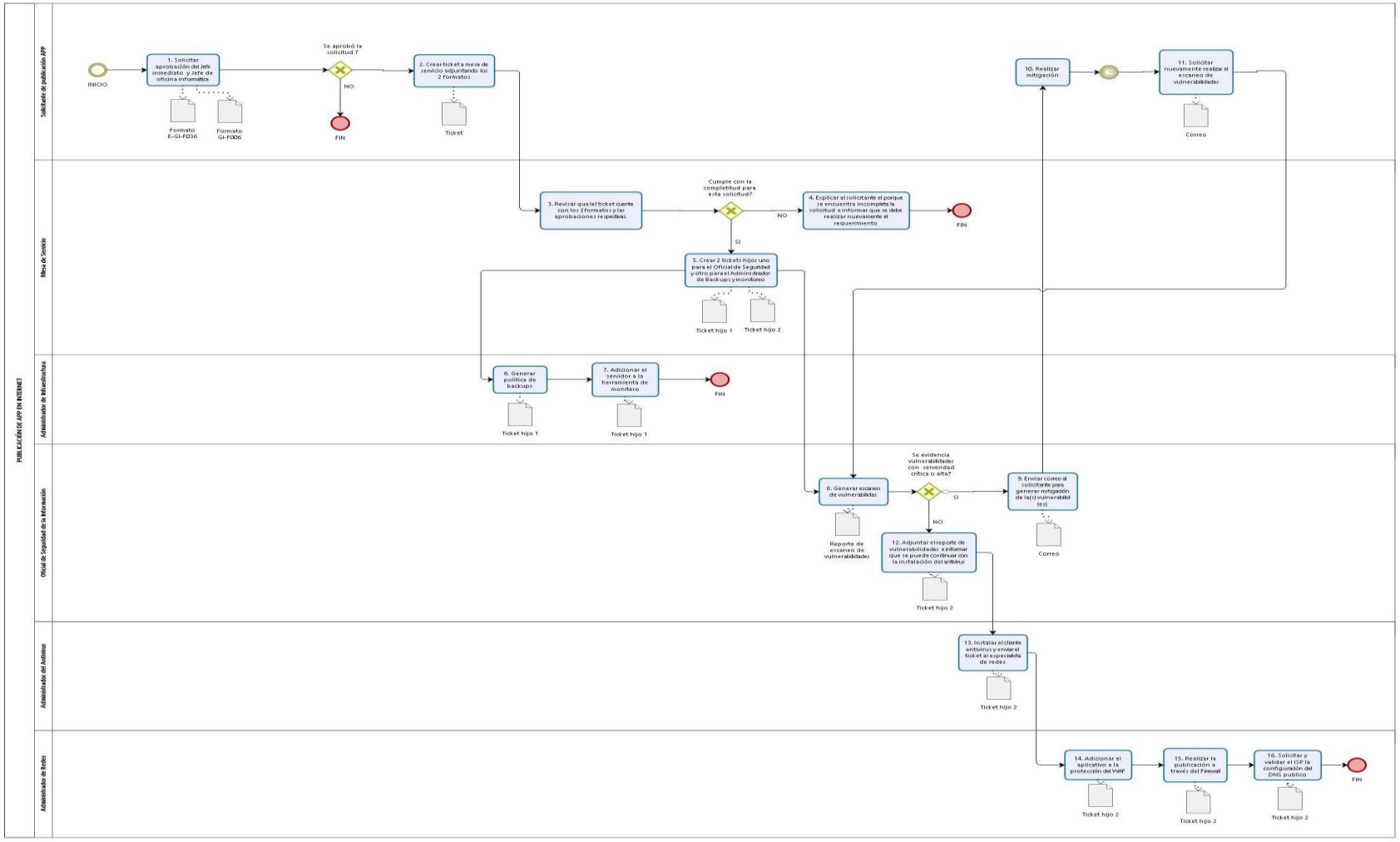
- ✓ Los controles para su publicación son los siguientes:
  - Generar política de Backups.
  - Adición a la herramienta de monitoreo.
  - Escaneo de vulnerabilidades.
  - Instalación del antivirus.
  - Publicación a través del WAF y FIREWALL.

- ✓ Las vulnerabilidades de seguridad con severidad crítica deberán ser mitigadas antes de publicar la aplicación.

6. ACTIVIDADES

No.	ACTIVIDAD	RESPONSABLE	REGISTRO
1	Solicitar aprobación del Jefe inmediato y Jefe de la oficina de informática, para ello se debe contar con 2 formatos E-GI-F036 y GI-F006 revisados y aprobados. De ser aprobados continuar con la actividad 2.	• Solicitante	• Dos Formatos
2	Crear ticket a mesa de servicio adjuntando los 2 formatos formatos E-GI-F036 y GI-F006.	• Solicitante	• Ticket
3	Revisar que el ticket cuente con los 2 formatos y las aprobaciones respectivas. De no contar con los formatos diligenciados y aprobaciones respectivas continuar con la actividad 4, de lo contrario continuar con la actividad 5.	• Mesa de Servicio	• Ticket
4	Explicar al solicitante por qué se encuentra incompleta la solicitud e informar que se debe realizar nuevamente el requerimiento	• Mesa de Servicio	• Ticket
5	Crear 2 tickets hijos, uno será asignado al Oficial de Seguridad y el otro para el Administrador de Backups y monitoreo.	• Mesa de Servicio	• Ticket
6	Generar política de Backups	• Administrador de Backups	• Ticket
7	Adicionar el servidor a la herramienta de monitoreo	• Administrador de monitoreo	• Ticket y herramienta Zabbix
8	Generar escaneo de vulnerabilidades, si no presenta vulnerabilidades críticas o altas continuar con la actividad 12 de lo contrario continuar con la actividad 9.	• Oficial de Seguridad de la Información	• Ticket y reporte de escaneo de vulnerabilidades
9	Enviar correo al solicitante para generar mitigación de la(s) vulnerabilidad(es)	• Oficial de Seguridad de la Información	• Correo y ticket
10	Realizar mitigación	• Solicitante	
11	Solicitar nuevamente realizar el escaneo de vulnerabilidades	• Solicitante	• Correo
12	Adjuntar el reporte de vulnerabilidades e informar que se puede continuar con la instalación del antivirus	• Oficial de Seguridad de la Información	• Ticket y reporte de vulnerabildiades
13	Instalar el cliente antivirus y enviar el ticket al especialista de redes	• Administrador del Antivirus	• Ticket
14	Adicionar el aplicativo a la protección del WAF	• Administrador Redes	• Ticket
15	Realizar la publicación a través del Firewall	• Administrador Redes	• Ticket
16	Solicitar y validar el ISP la configuración del DNS publico	• Administrador Redes	• Ticket

7. FLUJOGRAMA



8. HISTORIAL DE CAMBIOS

VERSIÓN	FECHA	DESCRIPCIÓN
01	05/02/2019	Creación del Procedimiento.

ELABORÓ:	REVISÓ:	APROBÓ:
Luis Alejandro Pinilla **Oficial de Seguridad de la Información**	Leonardo Cárdenas Chitiva **Jefe Oficina Informática**	Leonardo Cárdenas Chitiva **Jefe Oficina Informática**