1. **PROCESO:** Gestión de las Tecnologías de la Información.

2. **SUB PROCESO: N/A**

3. **OBJETIVO:** Definir los parámetros para que la autorización de instalación de software se realice de acuerdo a lo establecido en las políticas de seguridad de la información del SGSI.

4. **ALCANCE:** Inicia con la solicitud de aprobación de software y finaliza con su instalación.

5. **DISPOSICIONES GENERALES:**

Todo software que se instale en USPEC debe cumplir con una serie de aspectos que se exigen en las políticas de seguridad de la información; cada uno de éstos debe ejecutar los controles requeridos para mitigar los riesgos asociados con las vulnerabilidades que pueden surgir en el software, con base en las mejores prácticas de seguridad de la información. Los aspectos incluidos para este procedimiento son:

- ✓ **Justificación:** Verificar que la funcionalidad del software requerido esté plenamente justificada por la caracterización de un proceso formal dentro de USPEC.
- ✓ **Política de Desarrollo seguro:** Verificar que se cumpla con la Política de Desarrollo Seguro, donde se describen las directrices para el desarrollo de software.
- ✓ **Soporte:** Determinar cuál es el soporte requerido para el funcionamiento del software, estableciendo que se cubran los horarios de funcionamiento, los tiempos de respuesta y si este servicio se hará por parte de personal interno o lo hace una empresa encargada. Se debe validar que se cuente con el personal idóneo para dar soluciones a posibles problemas o incidentes de seguridad de la información.
- ✓ **Gestión de vulnerabilidades:** Verificar las vulnerabilidades asociadas con el sistema o aplicación, identificando proactivamente los puntos débiles que van siendo descubiertos con el tiempo y que deben ser corregidos oportunamente para prevenir los riesgos que puedan generarse.
- ✓ **Licenciamiento:** Aplicar el procedimiento de verificación de derechos de autor para el software que se requiere instalar.
- ✓ **Monitoreo:** Definir cuáles son los mecanismos para la detección de incidentes de seguridad de la información durante la operación del software que se requiere instalar.

6. **DEFINICIONES:**

Activo: Cualquier elemento que tiene valor para la organización y que para Gestión de riesgos de seguridad de la información se consideran los siguientes tipos: información, actividades y procesos del negocio, software, hardware, personal, redes, organización y ubicación.

Amenaza: Causa potencial de incidente no deseado, el cual puede resultar en daño al sistema o a la Organización. [Fuente: ISO 27000].

Confidencialidad: Propiedad de la información que hace que no esté disponible o que sea revelada a individuos no autorizados, entidades o procesos.

Disponibilidad: Propiedad de ser accesible y utilizable ante la demanda de una entidad autorizada. [Fuente: ISO 27000].

Importancia del activo: Valor que refleja el nivel de protección requerido por un activo de información frente a las tres propiedades de la seguridad de la información: integridad, confidencialidad y disponibilidad.

Integridad: Propiedad relacionada con la precisión y completitud.

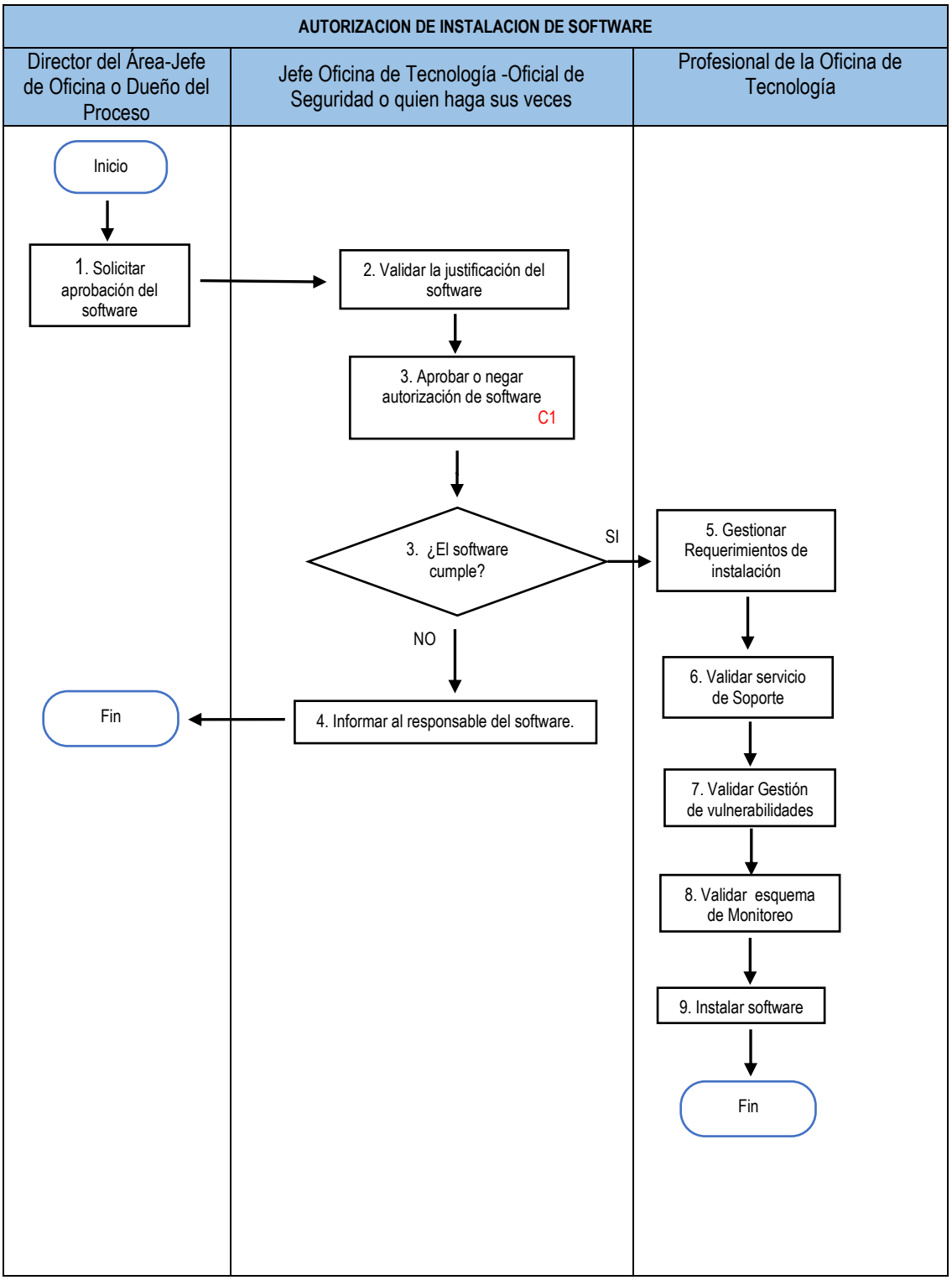
Monitoreo: Verificación, supervisión, observación crítica o determinación continúa del estado, con el fin de identificar cambios con respecto al nivel de desempeño exigido o esperado.

Propietario del activo: Persona o cargo que administra, autoriza el uso, regula o gestiona el activo de información. El propietario del activo aprueba el nivel de protección requerido frente a la confidencialidad, integridad y disponibilidad.

Riesgo: Efecto de la incertidumbre sobre los objetivos. Un efecto es una desviación de aquello que se espera, sea positivo, negativo o ambos. Los objetivos pueden tener aspectos diferentes (económicos, de imagen, medio ambiente) y se pueden aplicar a niveles diferentes (estratégico, operacional, toda la organización).

Vulnerabilidad: Debilidad identificada sobre un activo y que puede ser aprovechado por una amenaza para causar una afectación sobre la confidencialidad, integridad y/o disponibilidad de la información.

7. FLUJOGRAMA:



8. DESCRIPTIVO DEL PROCEDIMIENTO:

N°	Responsable	Registros	D Descripción de la actividad. Cx Punto de Control.	
1	Director del Área-Jefe de Oficina o Dueño del proceso	G1-S1-FO-04 Memorando	D	**Solicitar aprobación del software** Definir la información requerida para la aprobación del software, justificando la necesidad de instalación de acuerdo a las actividades o funciones desarrolladas dentro de los procesos de la USPEC.
2	Jefe Oficina de Tecnología - Oficial de Seguridad o quien haga sus veces.	A3-S1-FO-08 Autorización de Software	D	**Validar la justificación del software** Verificar que la funcionalidad del software corresponda a actividades justificadas por la caracterización de un proceso formal dentro de USPEC. De acuerdo al requerimiento, se validan las condiciones de instalación
3	Jefe Oficina de Tecnología - Oficial de Seguridad o quien haga sus veces	A3-S1-FO-08 Autorización de Software	D C1	**Aprobar o negar autorización del software** Si todos los aspectos exigidos son cumplidos por el software, en evaluación se autoriza la instalación. ¿El software cumple? **SI:** Continua con la actividad 5 **No**: Pasa a la actividad 4.
4	Jefe Oficina de Tecnología Oficial de Seguridad o quien haga sus veces	Correo electrónico	D	**Informar al responsable de la solicitud.** Mediante correo electrónico se informa al Director del Área-Jefe de Oficina o Dueño del proceso, explicando la razón por la que el software no se puede autorizar para ser instalado. Finaliza el procedimiento.
5	Profesional de la Oficina de Tecnología	Correo Electrónico	D	**Gestionar requerimientos de instalación.** Se notifica mediante correo electrónico a la Oficina de Tecnología, solicitando gestionar los requerimientos de instalación del software.
6	Profesional de la Oficina de Tecnología	A3-S1-FO-08 Autorización de Software	D	**Validar servicio de soporte** Se valida que el servicio de soporte definido corresponda al requerido durante la operación del software para cumplir con las Políticas de Seguridad de la información.

N°	Responsable	Registros	D Descripción de la actividad. Cx Punto de Control.	
7	Profesional de la Oficina de Tecnología	A3-S1-FO-08 Autorización de Software	**D**	**Validar la Gestión de vulnerabilidades** Se verifica que el software esté cubierto por un sistema de Gestión de Vulnerabilidades alineado con el SGSI de USPEC.
8	Profesional de la Oficina de Tecnología	A3-S1-FO-08 Autorización de Software	**D**	**Validar esquema de monitoreo** Se valida que el software durante su operación estará monitoreado para alinearse con la gestión de incidentes requerida por el SGSI de USPEC.
9	Profesional de la Oficina de Tecnología	A3-S1-FO-08 Autorización de Software Correo Electrónico	**D**	**Instalar software** Se realiza la instalación del software con base en las recomendaciones del fabricante. Una vez, haya sido instalado, se informa mediante correo electrónico al Director del Área-Jefe de Oficina o Dueño del proceso. Finaliza el procedimiento.

9. PUNTOS DE CONTROL:

Punto de Control	Responsable	Registro
C1 Verificar que la solicitud cumpla con los requisitos establecidos (disposiciones generales).	Jefe Oficina de Tecnología Oficial de Seguridad o quien haga sus veces	A3-FO-08 Autorización de Software

RESUMEN DE CAMBIOS:

Versión	Fecha	Numerales	Descripción de la modificación
01	30/08/2016	Todos	Se crea el documento

RESPONSABILIDAD Y AUTORIDAD		
Elaboró / Actualizó:	**Revisó:**	**Aprobó:**
Firma: Original Firmado	Firma: Original Firmado	Firma: Original Firmado
Nombre: Fernando Aguilera	Nombre: Camilo Alejandro Romero González	Nombre: Diana Lucia Pinilla Marín
Cargo: Consultor Externo - Globaltek Security SAS	Cargo: Analista de Sistemas	Cargo: Jefe Oficina de Tecnología
Dependencia: NA	Dependencia: Oficina de Tecnología	Dependencia: Oficina de Tecnología