1. OBJETIVO

Establecer las actividades para gestionar los requerimientos de validación de eventos de seguridad del Centro de Operaciones de Seguridad - SOC, mediante herramientas de administración de eventos e información que se encuentren bajo la gobernabilidad del proceso de gestión TIC, con el fin de identificar y evaluar amenazas para mitigar los impactos negativos en la información y las operaciones de la Entidad.

2. ALCANCE

Aplica tanto a los responsables internos como a los externos del Centro de Operaciones de Seguridad (SOC). Comienza con la configuración de casos de uso en el Sistema de Gestión de Eventos e Información de Seguridad (SIEM) y culmina con la ejecución de las recomendaciones por parte de los siguientes roles (Contratistas): Analista SOC, Oficial de Seguridad y Especialista en Soporte Antivirus Institucional .

La capacidad de correlación depende de la capacidad de procesamiento de cada herramienta SIEM institucional y de las licencias adquiridas en términos de Eventos por Segundo (EPS), así como de la vinculación de equipos a correlacionar en el SIEM y de la identificación de activos de información considerados críticos.

3. DEFINICIONES Y SIGLAS

ACL (Access Control List): lista de control de acceso es un informe sobre los permisos o derechos de acceso que tiene cada usuario sobre un objeto determinado.

Activo de información: en relación con la seguridad de la información, es cualquier información o elemento relacionado con el tratamiento de esta (sistemas, soportes, edificios, personas, etc.) que tenga valor para la organización.[1]

Bots Maliciosos: programas automatizados diseñados para llevar a cabo actividades dañinas o no autorizadas en sistemas informáticos y redes. Estos bots pueden ejecutar ataques como la saturación de servicios mediante DDoS (ataques distribuidos de denegación de servicio), el envío masivo de correos no deseados (spam), el robo de datos sensibles, la distribución de malware o la suplantación de identidad en plataformas en línea. Generalmente operan como parte de redes organizadas llamadas botnets, que son controladas por actores malintencionados para realizar estas actividades a gran escala, comprometiendo la seguridad de los sistemas y la privacidad de las personas.

Caso de Uso: se refiere a un escenario específico en el que se define cómo deben ser monitoreados y gestionados ciertos eventos de seguridad en un sistema, servicio o red de comunicaciones, que indica una posible violación de la política de seguridad de la información o falla de los controles, o una situación previamente desconocida que puede ser relevante para la seguridad de la información. Esto puede incluir la detección de amenazas, el cumplimiento normativo y la automatización con inteligencia artificial.

[1]Modelo de Seguridad y Privacidad de la Información del MinTIC, febrero de 2021.

Correlación de eventos: función clave de las herramientas SIEM, que procesan los registros generados continuamente por dispositivos y aplicaciones en la red. Mediante reglas de correlación, el SIEM identifica secuencias de eventos que podrían indicar anomalías, como vulnerabilidades de seguridad o ataques cibernéticos, detectando patrones y relaciones entre eventos aparentemente no relacionados. Para lograrlo, aplica inteligencia a los datos recibidos de los activos, permitiendo identificar comportamientos sospechosos. Sin embargo, la calidad de esta correlación depende de la integración con todas las fuentes relevantes, como registros de firewall, servidores y aplicaciones; a mayor cantidad de información disponible, mejor será la capacidad de detección de la herramienta.

Evento de seguridad de la información: ocurrencia identificada en un sistema, servicio o red que indica una posible brecha de seguridad, falla de un control o una condición no identificada relevante para la seguridad de la información.

Firewall-FW: o cortafuegos es un sistema de seguridad diseñado para bloquear accesos no autorizados a una red o a un ordenador, mientras permite la comunicación con servicios autorizados. Funciona como una barrera que filtra el tráfico de datos, permitiendo solo el paso de aquellos que cumplen con ciertos criterios de seguridad.

Hash: cadena de caracteres de longitud fija generada a partir de datos de entrada mediante una función hash criptográfica. Se utiliza para verificar la integridad y autenticidad de los datos, asegurando que no han sido alterados.

Impacto: costo que enfrenta una organización debido a un evento, independientemente de su escala, el cual puede evaluarse más allá de términos estrictamente financieros. Incluye aspectos como pérdida de reputación, implicaciones legales, interrupciones operativas y otros efectos que pueden afectar su estabilidad o desempeño.

Incidente de seguridad de la información: (Inglés: Information security incident). Evento único o serie de eventos de seguridad de la información inesperados o no deseados que poseen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información.

Indicadores de compromiso (IoC): evidencias que sugieren que un sistema ha sido comprometido o está siendo objeto de un ataque. Estos pueden incluir direcciones IP maliciosas, nombres de archivos sospechosos, hashes de archivos, URLs, y otros datos técnicos que permiten identificar actividad malintencionada o anomalías en el entorno.

IP: (Protocolo de Internet, por sus siglas en inglés) es un identificador único asignado a cada dispositivo conectado a una red, como computadoras, teléfonos o servidores, que permite que estos se comuniquen entre sí. Funciona como la "dirección" del dispositivo en internet o en una red local, lo que facilita el envío y recepción de datos.

Logs: registros detallados de eventos generados por sistemas, aplicaciones o dispositivos, que documentan actividades como errores, advertencias, transacciones y datos de depuración. En el contexto de la seguridad de la información digital, los logs son esenciales para solucionar problemas, realizar análisis de rendimiento y detectar posibles vulnerabilidades o amenazas.

Mesa de servicio: centro de soporte que provee un único punto de contacto con los usuarios para atender los requerimientos e incidentes de acuerdo con los niveles de escalamiento.

Playbook: conjunto de herramientas, condiciones, lógica de negocio, flujos y tareas utilizadas para responder a sucesos y amenazas de seguridad en un entorno SOAR.

Política de Seguridad de la Información: documento de alto nivel que refleja el compromiso de la administración con la seguridad de la información y establece lineamientos y procedimientos a implementar para su gestión.

PROVEEDOR: Contratista o Tercero, cuando aplique.

Registros de eventos: en el contexto del SIEM es un conjunto de datos detallados que captura y documenta las actividades y eventos ocurridos en los dispositivos y sistemas de una red. Estos registros incluyen información sobre accesos, intentos de intrusión, cambios en configuraciones, alertas de seguridad, y otros eventos relacionados con la seguridad.

Reputación de la IP: medida de la confiabilidad y comportamiento de una dirección IP en línea. Los proveedores de servicios de internet (ISP) utilizan esta reputación para evaluar si una IP ha estado involucrada en actividades maliciosas, como el envío de spam, conexiones sospechosas o relaciones con bots y fraudes. Una IP con historial negativo puede ser incluida en listas negras, mientras que una con un buen historial puede aparecer en listas blancas. En el contexto de un SIEM, la reputación de la IP ayuda a identificar comportamientos anómalos que podrían indicar amenazas o actividades maliciosas, tanto internas como externas, a través de la monitorización y correlación de eventos en la red.

SIEM (Security Information and Event Management): solución de seguridad que permite la recopilación, monitoreo, análisis y gestión de datos relacionados con eventos y actividades de seguridad en una red o sistema. Su objetivo principal es detectar, identificar y responder a amenazas cibernéticas, así como garantizar la integridad, confidencialidad y disponibilidad de la información. Un SIEM centraliza los registros de eventos (logs) provenientes de diferentes fuentes, como sistemas, aplicaciones y dispositivos de red, para realizar correlaciones, análisis en tiempo real y generar alertas ante posibles incidentes de seguridad.

SOAR (Security Orchestration, Automation, and Response - Orquestación, Automatización y Respuesta de Seguridad)**:** conjunto de herramientas y servicios diseñados para automatizar la prevención y respuesta ante ciberataques. Integra y coordina diversas actividades para que las organizaciones puedan responder de manera rápida y eficiente a las amenazas. Funciona en conjunto con el SIEM, procesando los eventos de seguridad ya recopilados y proporcionando análisis automatizados para priorizar y gestionar dichos eventos. En resumen, SOAR ayuda a los equipos de seguridad a automatizar la respuesta a incidentes, mejorando la eficacia y velocidad en la gestión de amenazas.

SOC (Security Operation Center – Centro de Operaciones de Seguridad): encargado del monitoreo, seguimiento y análisis de las actividades de las redes de datos, servidores, bases de datos, aplicaciones o sitios web, con el fin de identificar actividades anómalas que puedan indicar eventos o compromisos de seguridad informática.

Triage: proceso mediante el cual un evento es valorado con el fin de determinar la urgencia

del evento, designar los recursos y priorizar la atención o respuesta.

URL (Uniform Resource Locator): dirección única que se utiliza para localizar un recurso en internet, como una página web, una imagen, un video o un archivo. La URL especifica el protocolo a utilizar (como *http* o *https*), el dominio o dirección del servidor donde se encuentra el recurso, y, en muchos casos, la ruta y el nombre del archivo o recurso dentro de ese servidor.

4. MARCO LEGAL / DOCUMENTOS DE REFERENCIA

Decreto 767 de 2022; mediante el cual se actualizó la política de Gobierno Digital del país

Política de seguridad de la Información y Seguridad Digital de la FGN vigente.

Buenas prácticas basadas en los estándares nacionales e internacionales aplicables a la entidad en materia de seguridad de la información digital.

5. DESARROLLO

5.1 Crear/modificar/eliminar Caso de uso

No.	ACTIVIDAD Y DESCRIPCIÓN	RESPONSABLE	REGISTRO
5.1.1	**Desarrollo Casos de Uso** **a. Análisis y configuración de Casos de Uso en el SIEM** Definir si se trata de una creación de caso de uso, una actualización o la eliminación. Para la creación del caso de uso, se debe identificar la necesidad específica para la cual se requiere gestionar una alerta, estableciendo: Activo de información. Descripción del evento o necesidad de acción que origina la alerta. Determinar puertos o direcciones (origen y destino) en el que se genera el evento. Tipo de solicitud.	Analista SOC-PROVEEDOR	Mesa de Servicios de la FGN
	b. Sustentación de la necesidad para la modificación de casos de uso. Validar la procedencia de la solicitud para autorizar o no la creación, modificación o eliminación del caso de uso.	Analista SOC-PROVEEDOR	

No.	ACTIVIDAD Y DESCRIPCIÓN	RESPONSABLE	REGISTRO
	c. Realizar un análisis inicial identificando: Actores o ejecutantes. Dueños de los activos. Formulación de plan de acción con las posibles acciones a implementar. (Bloquear, suspender, escanear, cuarentena - aislar etc.) Descripción de capacidad de respuesta evaluando la criticidad y el impacto del evento. Necesidad de escalamiento (al dueño del activo o al oficial de seguridad) por tratarse de un evento que sea un posible incidente de seguridad.	Analista SOC-PROVEEDOR	
	d. Registro en Mesa de Servicios Una vez identificada la necesidad de correlación de un equipo o creación de una alerta, se crea el caso en la herramienta de Mesa de Servicios de la Entidad y analiza el requerimiento para configurar el caso de uso en el SIEM.	Analista SOC-PROVEEDOR	
	e. Verificar la configuración del SIEM Verificar y viabilizar que se requiere ajustar para que sea autorizada la creación, modificación o eliminación del caso de uso correspondiente a la necesidad de monitoreo y alerta con mínimo: Rangos de monitoreo, como es el caso del número de hits o unidades desde el cual se debe alertar. Tipos de Eventos. Destino de la Alerta.	Analista SOC-PROVEEDOR	
	f. Autorización de la Actualización del Caso de Uso El especialista de seguridad (líder de operaciones de seguridad) del SOC de la FGN, analiza el objetivo de la solicitud para **autorizar o no la creación, modificación o eliminación** del caso de uso.	Líder SOC de la FGN	SIEM y Mesa de Servicios FGN
	g. Refinamiento o ajuste Dar autorización de crear, modificar o eliminar el caso de uso en el SIEM. Posteriormente, verificar su funcionamiento y aprobar la acciones	Analista SOC-PROVEEDOR	Mesa de Servicios de la FGN

Puntos de control

No. de la Actividad	Que Evento Controla	Responsable	Registro

5.1.1	**b. Sustentación de la necesidad para la modificación de casos de uso.** Analizar el propósito de la solicitud sobre el caso de uso.	Analista SOC-PROVEEDOR	Mesa de servicios FGN
5.1.1	**e. Verificar la configuración del SIEM** Configurar el caso de uso de manera que responda al evento de manera eficiente.	Analista SOC-PROVEEDOR	Mesa de servicios FGN
5.1.1	**f. Autorización de la Actualización del Caso de Uso** El especialista de seguridad (líder de operaciones de seguridad) del SOC de la FGN, analiza el objetivo de la solicitud para autorizar o no la creación, modificación o eliminación del caso de uso.	Líder SOC de la FGN	SIEM y Mesa de Servicios FGN

Ver ANEXO 1.

5.2. Creación/Modificación/Eliminación de PlayBook SOAR

No.	ACTIVIDAD Y DESCRIPCIÓN	RESPONSABLE	REGISTRO
5.2.1.	**Desarrollo de Playbook en** **Verificación de configuración:** **Validar la configuración del SOAR**. En caso de determinar su necesidad y viabilidad, debe registrar un caso acompañado de la documentación correspondiente del Playbook que se requiere crear, ajustar o eliminar, con el fin de gestionar su autorización para la creación, modificación o eliminación del mismo.	Analista SOC-PROVEEDOR	Mesa de Servicios de la FGN
5.2.2.	**Evaluación** El Especialista de Seguridad de la FGN es responsable de **autorizar la creación, modificación o eliminación del Playbook en el SOAR**. En caso de no aprobar la solicitud, debe justificar la decisión indicando las razones de la no aprobación, y, si es necesario, requerir información adicional o proceder al cierre del caso.	Líder SOC-FGN	Mesa de Servicios de la FGN

No.	ACTIVIDAD Y DESCRIPCIÓN	RESPONSABLE	REGISTRO
5.2.3.	**Acciones y ajustes** El Analista SOC del proveedor, **crea, modifica o elimina el *Playbook* en el SOAR** y documenta el caso.	Analista SOC-PROVEEDOR	SOAR y Mesa de Servicios de la FGN

Puntos de control

No. de la Actividad	Que Evento lo Controla	Responsable	Registro
5.2.2	Evaluación Autorizar creación, modificación o eliminación del *Playbook* en el SOAR	Líder SOC-FGN	Mesa de Servicios de la FGN

Ver ANEXO 2.

5.3. Validación de Eventos

No.	ACTIVIDAD Y DESCRIPCIÓN	RESPONSABLE	REGISTRO
5.3.1.	**Realización de concepto o recomendación** de acuerdo con el triage realizado por el SIEM, el operador del SOC selecciona, eventos con prioridad alta para su revisión, considerando los siguientes aspectos: Reputación de las IPs La revisión de *logs* en busca de posibles eventos de seguridad. Verificar si el antivirus está instalado en las máquinas institucionales con las direcciones detectadas (accede a la consola del antivirus y comprueba su estado si está instalado o no). **Emite el concepto o las recomendaciones** en el formulario de la herramienta definida para este fin. Generar casos en Mesa de servicios con el concepto o las recomendaciones para Analista SOC del proveedor.	Operador SOC-FGN	Mesa de Servicios de la FGN

No.	ACTIVIDAD Y DESCRIPCIÓN	RESPONSABLE	REGISTRO
5.3.2.	**Validación Recomendación** Verifica las recomendaciones emitidas por el Operador SOC de la FGN. Si considera necesario realizar una nueva revisión, escala nuevamente el caso al Operador SOC de la FGN para que lleve a cabo la verificación correspondiente. Las acciones básicas a implementar consisten en: Bloqueo (listas de bloqueo). Listas blancas (desestimación o Monitoreo). Actualización de indicadores de compromiso (Hash).	Analista SOC-PROVEEDOR	Mesa de Servicios de la FGN
5.3.3	**Ejecución Recomendación** Los responsables deben ejecutar la recomendación y validar las acciones implementadas. 1.IP's adicionadas a listas de bloqueo/blancas en el SIEM 2. IP's adicionadas a listas de bloqueo/blancas en el Firewall 3.Validar Antivirus instalado y actualizado y generar escaneo bajo demanda en los equipos	1.Analista SOC-PROVEEDOR 2. Oficiales de Seguridad del proveedor 3. Soporte Antivirus Institucional.	SIEM FIREWALL ANTIVIRUS

Puntos de control

No. de la Actividad	Acciones a realizar	Responsable	Registro
5.3.2.	**Validación de la recomendación** Autorizar la adición de la IP a Listas Negras o de Bloqueo o listas Blancas por parte de los actores responsables o solicitar la corrección de la recomendación	Analista SOC-PROVEEDOR	Mesa de Servicios de la FGN

Ver ANEXO 3.

5.4.Reportes SIEM

No.	ACTIVIDAD Y DESCRIPCIÓN	RESPONSABLE	REGISTRO
5.4.1	**Realización de la Solicitud** Son los diferentes reportes que se pueden obtener de acuerdo con los dispositivos correlacionados en la plataforma SIEM. El usuario crea un caso Alarmas SIEM/Reporte de	Operador SOC-FGN	Mesa de Servicios de la FGN

No.	ACTIVIDAD Y DESCRIPCIÓN	RESPONSABLE	REGISTRO
	eventos de seguridad de entrega de reportes solicitados por demanda en Mesa de Servicios, quien debe validar que el usuario haya adjuntado al caso la(s) IP, nombre dispositivos que desea consultar (correlacionar), o el nombre de la alarma. El Especialista de Seguridad de la FGN, registra caso en la Mesa de Servicios con la (s) IP(s) y dispositivos o nombre de las alarmas de la Mesa de Servicios.		
5.4.2.	**Análisis del requerimiento:** **Verificar** que la información enviada contenga la IP, nombres de dispositivos o nombre de las alarmas correctamente para poder generar el reporte.	Analista SOC-PROVEEDOR	Mesa de Servicios de la FGN
5.4.3.	**Realización del requerimiento:** Realizar reportes por demanda	Analista SOC-PROVEEDOR	Mesa de Servicios de la FGN

PUNTOS DE CONTROL

No. de la Actividad	Que Evento lo Controla	Responsable	Registro
5.4.2.	Verificar Generación y entrega de reportes por demanda	Analista SOC-PROVEEDOR	Mesa de Servicios de la FGN

Ver ANEXO 4.

5.5.Gestión de Indicadores de Compromiso.

No.	ACTIVIDAD Y DESCRIPCIÓN	RESPONSABLE	REGISTRO
5.5.1.	**Recolección de la Información.** Validar la información: Se identifica en las diferentes fuentes los posibles indicadores de compromiso a implementar en la consola Antivirus institucional, antivirus perimetral, en la Plataforma SIEM y SOAR y en el FireWall (FW) y coloca el caso en la herramienta de Mesa de Servicios de la Entidad. Identificar en las plataformas SIEM y SOAR los posibles indicadores de compromiso a implementar en el Firewall y en la consola Antivirus institucional	Especialista de seguridad FGN Analista SOC-PROVEEDOR	Mesa de Servicios de la FGN

No.	ACTIVIDAD Y DESCRIPCIÓN	RESPONSABLE	REGISTRO
5.5.2.	Desarrollo de la Solución: De **Adicionar hash** Adicionar indicadores de compromiso en la Consola de ● Antivirus institucional ● Antivirus perimetral **Adicionar indicadores de compromiso**: ● en la plataforma perimetral(Firewall-FW) ● En el SIEM Documentación y cierre del caso en Mesa de Servicios de la FGN.	Especialista de Antivirus Institucional (soporte de antivirus). Oficial de Seguridad - PROVEEDOR Analista SOC-PROVEEDOR	Mesa de Servicios de la FGN.
5.5.3.	**Validación de la Solución:** Constata las evidencias de incorporación del IoC (HASH, IP, etc). Documentación en Mesa de Servicios de la FGN.	Especialista de seguridad FGN	Mesa de Servicios de la FGN.

Puntos de control

No. de la Actividad	Que Evento lo Controla	Responsable	Registro
5.5.3.	Validar Solución Registra la solución realizada por cada responsable.	Especialista de seguridad FGN	Mesa de Servicios de la FGN

Ver ANEXO 5.

5.6.ACL

No.	ACTIVIDAD Y DESCRIPCIÓN	RESPONSABLE	REGISTRO
5.6.1	**Validación del Requerimiento.** El usuario de la FGN (funcionales, administradores, etc) solicitan permisos de acceso a sistemas de información (ACL) creación, modificación y eliminación, para abrir los puertos para la comunicación entre Sedes o sede/aplicación.Debe ingresar la información requerida en el formulario de Mesa de Servicios: IP Origen, IP destino, Puertos y tipo (UDP o TCP), descripción del servicio, acción (permitir, denegar): Si el ACL es Nacional o Seccional, o es sede -aplicación, Vigencia :Permanente o temporal (hasta que fecha) y Observaciones: que se deban tener en cuenta o	Mesa de Servicios de la FGN Nivel 1 y 2	Mesa de Servicios de la FGN

No.	ACTIVIDAD Y DESCRIPCIÓN	RESPONSABLE	REGISTRO
	explicar con el fin de que los técnicos de soporte en sitio lo sepan, si tienen que hacer alguna instalación y para hacer las pruebas más adelante con el usuario) El usuario debe adjuntar el FORMATO ACUERDO DE CONFIDENCIALIDAD DE LA INFORMACIÓN del Proceso Gestión TIC y la información técnica que le hayan entregado para establecer la comunicación (manual técnico, información técnica, instalación de clientes etc.) Mesa de Servicios debe validar que el usuario adjunte el formato F17 completamente diligenciado en sus últimas versiones, y los campos de solicitud de ACL estén diligenciados para la solución en el formulario, además de la información técnica sea en un manual o indicaciones para que los Técnicos de Soporte en sitio, puedan realizar las pruebas y validar que el ACL esté bien configurado.		
5.6.2.	**Autorización ACL** Los especialistas de Seguridad de la FGN realizan las validaciones y autorizan o no la creación o modificación o eliminación de permisos, si no se autoriza se documenta la razón o se solicita más información o se cierra el caso. Si se autoriza se escala al grupo resolutor Oficiales de Seguridad del proveedor del servicio de seguridad perimetral para que realicen el requerimiento.	Especialista de seguridad FGN	Mesa de Servicios de la FGN.
5.6.3	**Solución del requerimiento:** Los miembros del Grupo resolutor Oficiales de Seguridad del proveedor: 1.Hacen la configuración y documentan las Listas de Control de Acceso de los equipos de la red nacional de comunicaciones de la Entidad. 2.Lo escalan a Mesa de Servicios (y estos a soporte en sitio) para que realicen las pruebas de acceso con el usuario quien conoce con qué credenciales va a ingresar (procedimiento si lo hay). Si el usuario puede acceder, se documenta el caso y se cierra, si no se devuelve a los agentes de Mesa de Servicios para que escalen al grupo resolutor oficiales de seguridad del proveedor para los respectivos ajustes.	Oficial de seguridad - PROVEEDOR	Mesa de Servicios de la FGN.

Puntos de control

No. de la Actividad	Que Evento lo Controla	Responsable	Registro
5.6.2	**Autorizar ACL** Valida que los formatos estén bien diligenciados y completos, la información requerida para configurar el ACL y la documentación técnica	Especialista de seguridad FGN	Mesa de Servicios de la FGN

Ver ANEXO 6.

5.7. Correo, Archivo o URL sospechoso

No.	ACTIVIDAD Y DESCRIPCIÓN	RESPONSABLE	REGISTRO
5.7.1.	**Validación de la solicitud:** el usuario debe anexar el respectivo correo, archivo o URL- Sospechoso. Nota: No se aceptan imágenes. Solo el mensaje con extensión .EML, si el usuario no sabe cómo anexar el respectivo archivo, correo o URL sospechosa, los Técnicos de Soporte en sitio deben apoyar para adjuntar la evidencia al caso.	Mesa de Servicios Nivel 1 y 2	Mesa de Servicios de la FGN.
5.7.2.	**Análisis y concepto** El Oficial de seguridad-PROVEEDOR que está resolviendo el caso debe realizar el análisis del correo, archivo o URL sospechoso con el fin de responder al usuario si es sospechoso o no, también debe realizar el concepto con las recomendaciones al grupo de Seguridad de la FGN para dar la autorización de bloquear, adicionar Hash o ambos.	Oficial de Seguridad - PROVEEDOR	Mesa de Servicios de la FGN.
5.7.3.	**Validación recomendación** De acuerdo al concepto del Oficial de seguridad-PROVEEDOR, el especialista de seguridad de la FGN autoriza o no realizar el bloqueo según la categoría correspondiente(de correo, Archivo o URL sospechosa), si no se autoriza, documenta y se cierra el caso. Si el concepto del Oficial de seguridad-PROVEEDOR es adicionar hash, el especialista de seguridad de la FGN autoriza o no realizar la adición de hash, si no autoriza, documenta el caso y se cierra.	Especialista de seguridad FGN	Mesa de Servicios de la FGN.

No.	ACTIVIDAD Y DESCRIPCIÓN	RESPONSABLE	REGISTRO
5.7.4.	**Ejecución recomendación** Después de ser autorizado: El oficial de Seguridad-PROVEEDOR procede al bloqueo, documenta y cierra el caso. El Soporte Antivirus: Realiza la actividad de Adicionar Hash, documenta y cierra el caso.	Oficial de Seguridad - PROVEEDOR Soporte de Antivirus Institucional	Mesa de Servicios de la FGN

Puntos de control

No. de la Actividad	Que Evento lo Controla	Responsable	Registro
5.7.2	**Análisis y concepto de archivo, correo o URL sospechoso** Verificación si el correo o Archivo o URL es o no sospechoso y de acuerdo al análisis el Oficial de seguridad-PROVEEDOR, realizará el concepto con una de las 3 las recomendaciones: realizar bloqueo y adicionar hash, Bloquear, Adicionar hash, cada una de estas acciones es autorizada por el Especialista Seguridad FGN	Oficial de seguridad - PROVEEDOR	Mesa de Servicios de la FGN

Ver ANEXO 7.

h. ASPECTOS GENERALES

Aplicación de registro y Gestión de casos:
La herramienta de registro para gestionar las solicitudes, permite centralizar y organizar la información, facilitando la comunicación y resolución por medio de un sistema de ***tickets*.**

Un *ticket* en el contexto de una Mesa de Servicios es un registro digital creado para documentar y gestionar una solicitud de soporte, un problema técnico o una pregunta de un usuario. Algunos componentes y funciones principales:

Número de Ticket: Un identificador único que permite rastrear el ticket a lo largo de su ciclo de vida.
Información del Cliente: Datos personales o de la empresa del usuario, como nombre y datos de contacto.
Detalles del Problema o Solicitud: Una descripción detallada del problema, incluyendo mensajes de error, capturas de pantalla y cualquier paso previo tomado para intentar resolverlo.
Prioridad y Estado: Indica la urgencia del ticket y su estado actual (abierto, en progreso, resuelto, etc.).

Historial de Actividades: Registro de todas las acciones y comunicaciones relacionadas con el ticket, lo que facilita el seguimiento y la colaboración entre agentes.

Los tickets son esenciales para organizar y priorizar las solicitudes, asegurando que cada problema reciba la atención adecuada y se resuelva de manera eficiente**.**

Alguna de las funciones principales son: Creación y Seguimiento de Tickets: Asignación Automática de *Tickets*, Prioridad y Categorías, Comunicación Centralizada, Historial y Registro de Actividades, Notificaciones y Alertas, Informes y Análisis

El registro se realiza a través de la Intranet/ SUSI: Aplicativo "**Mesa de Servicios**"

La gestión de casos también puede realizarse por medio de los siguientes canales:

Correo Electrónico: mesaserviciostic@fiscalia.gov.co
Línea Fija: (601) 7422733 Línea **Celular:** 3164373382
Línea 018000: 01800018994
Llamadas Externas: (601)5702000 extensión 5500
Línea Interna (marcación corta): extensión 5500

Capacidades y casos de uso de SIEM: Las capacidades de las herramientas SIEM varían, pero, en general, ofrecen las siguientes funciones principales:

Las herramientas SIEM recopilan grandes cantidades de datos en un solo lugar, los organizan y luego determinan si existen signos de amenaza, ataque o vulneración.
Los datos recolectados se clasifican para identificar relaciones y patrones en la herramienta SIEM con el fin de detectar amenazas potenciales y responder a ellas.
La herramienta SIEM monitorea los eventos de seguridad en la red y proporciona alertas y logs de la actividad relacionada con un evento.

Las herramientas SIEM generan alertas con base en los casos de uso configurados previamente por el Analista SOC para un análisis posterior.

Para crear un ***playbook*****,** el entorno SOAR se define del siguiente modo:

Orquestación: un entorno en el que las herramientas de seguridad y las soluciones pueden funcionar juntas para detectar, responder y ofrecer soluciones para sucesos y amenazas de seguridad.
Automatización: detección y respuesta a sucesos y amenazas sin intervención humana. Esto incluye la actualización de la respuesta a medida que el suceso progresa y se modifica.
Respuesta: procesos de métodos incorporados para responder y ofrecer soluciones a sucesos y amenazas.

Adición de Hash
La adición de hashes en el contexto del antivirus institucional permite una detección rápida y precisa de archivos maliciosos. Al comparar los hashes de los archivos en el sistema con una base de datos de hashes de malware conocido, el antivirus puede identificar y neutralizar

amenazas de manera eficiente. Además, los hashes aseguran la integridad de los archivos críticos del sistema, alertando sobre cualquier modificación no autorizada. Esta tecnología mejora significativamente la capacidad del antivirus para proteger los equipos institucionales, garantizando un entorno digital más seguro y confiable.
Los hashes se añaden al antivirus en varios momentos clave para garantizar una protección efectiva:
Durante las Actualizaciones de la Base de Datos: Los proveedores de antivirus actualizan regularmente sus bases de datos de hashes para incluir nuevos *malware*. Esto permite que el antivirus detecte y elimine las amenazas más recientes.
Al Escanear el Sistema: Cuando el antivirus realiza un escaneo, genera hashes para los archivos en el sistema y los compara con los de su base de datos. Si encuentra una coincidencia, identifica el archivo como malicioso.
Al Instalar o Actualizar Software: Algunos antivirus generan hashes para los archivos de software instalados o actualizados para asegurarse de que no han sido alterados por malware.
Verificación de Integridad: Los hashes se utilizan para verificar que los archivos críticos del sistema no hayan sido modificados. Si el hash de un archivo cambia, el antivirus puede alertar al usuario o tomar medidas para restaurar el archivo original.
Correos electrónicos sospechosos: pueden resultar muy convincentes gracias a la suplantación de marcas o personas y el uso de logotipos de marcas y un lenguaje formal. En un correo que le inciten a tomar medidas inmediatas que podrían revelar información privada. Algunas señales de advertencia en el correo para saber si no es real:

El nombre del remitente es vago y su dirección de correo es larga o complicada.
El asunto del correo es alarmista o busca llamar la atención.
El correo incita a algún tipo de acción inmediata.
Se ofrece un gran descuento como incentivo.
En el correo se utilizan pretextos para conseguir sus datos personales, incluida la información de inicio de sesión de algún sitio web.
En el correo se le incita a hacer clic en un hipervínculo sin aclarar adónde lleva.

URL sospechosa: Busca de igual manera suplantar una página web o un servicio, esto se conoce como Phishing, el usuario navega sobre una página identifica a la suplantada, normalmente se le solicita información como cuentas de usuario, contraseñas o información bancaria, esta información es entregada a los hackers que crearon el sitio "Falso". Para detectar un ataque phishing, hay que observar y comprobar:
Gramática y puntuación. Si un correo no está bien redactado o contiene faltas de ortografía es probable que no se trate de un comunicado profesional sino de un mensaje fraudulento.
Solicitud de información sensible.
Archivos adjuntos o vínculos.
Errores ortográficos.
Gráficos con aspecto poco profesional

Archivo Sospechoso: Es aquel que se camufla bajo la imagen de un archivo genuino (icono, nombre, extensión), esto con el fin de engañar al usuario y no desconfíe del archivo, el cual puede contener malware o software malicioso(virus, gusanos, troyanos) diseñado para infectar los dispositivos y que se ejecuta o activan, tan pronto el usuario abra el archivo que

por lo general solicitan contraseña para abrirlos. Una buena práctica es utilizar la Herramienta de eliminación de software malintencionado de Windows antes de abrirlo.

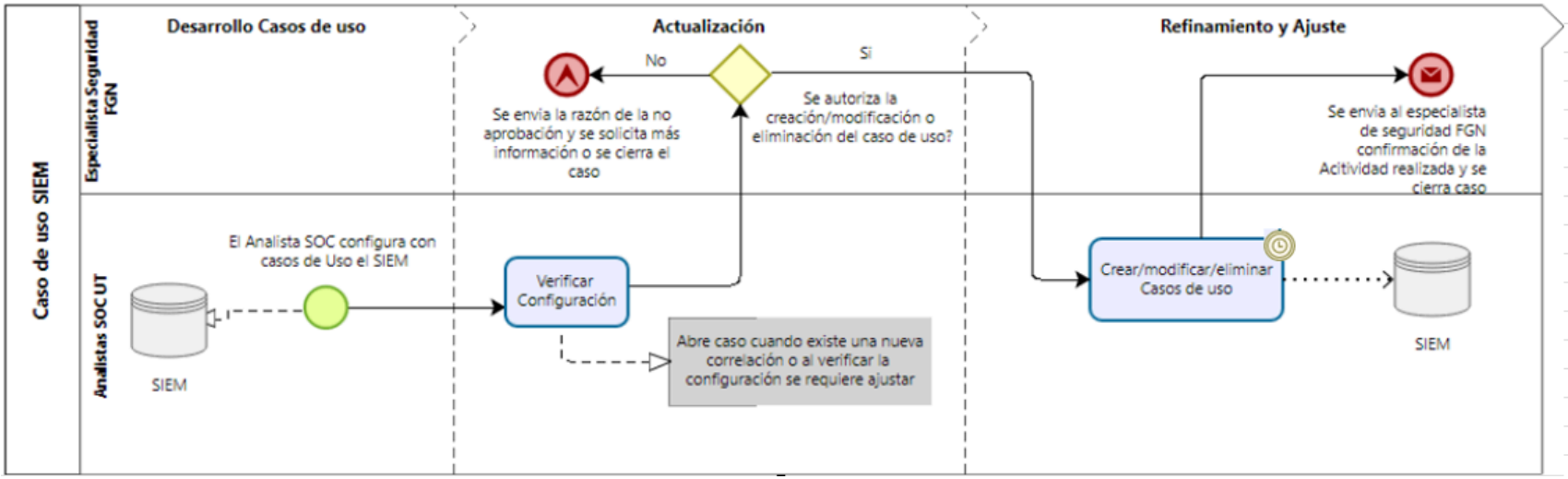
i. REVISIÓN Y APROBACIÓN

Revisó: Departamento de Arquitectura, Proyectos y Gobierno de TI, Grupo de Seguridad Digital y Ciberseguridad, Subdirección de Tecnologías de la Información y las Comunicaciones.

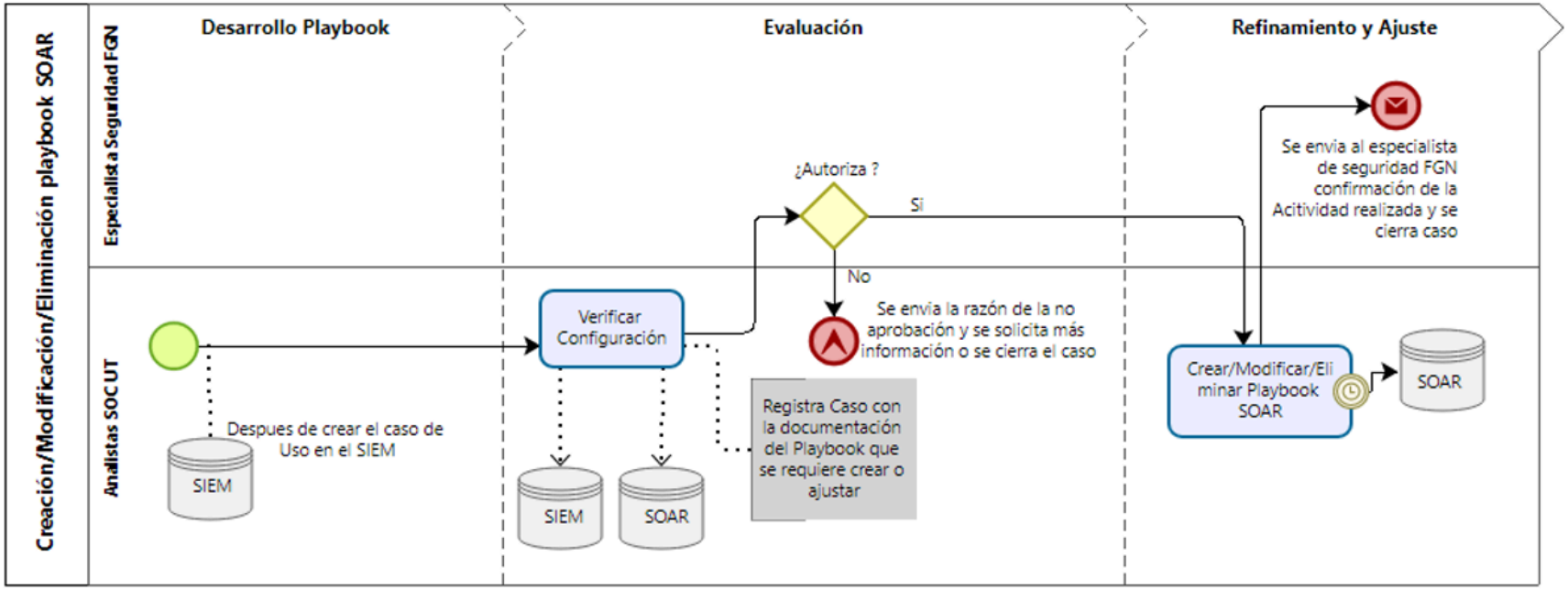
Aprobó: Líder del proceso Gestión TIC, Alejandra Torres Duque, Subdirectora Nacional de Tecnologías de la Información y las Comunicaciones

j. ANEXOS

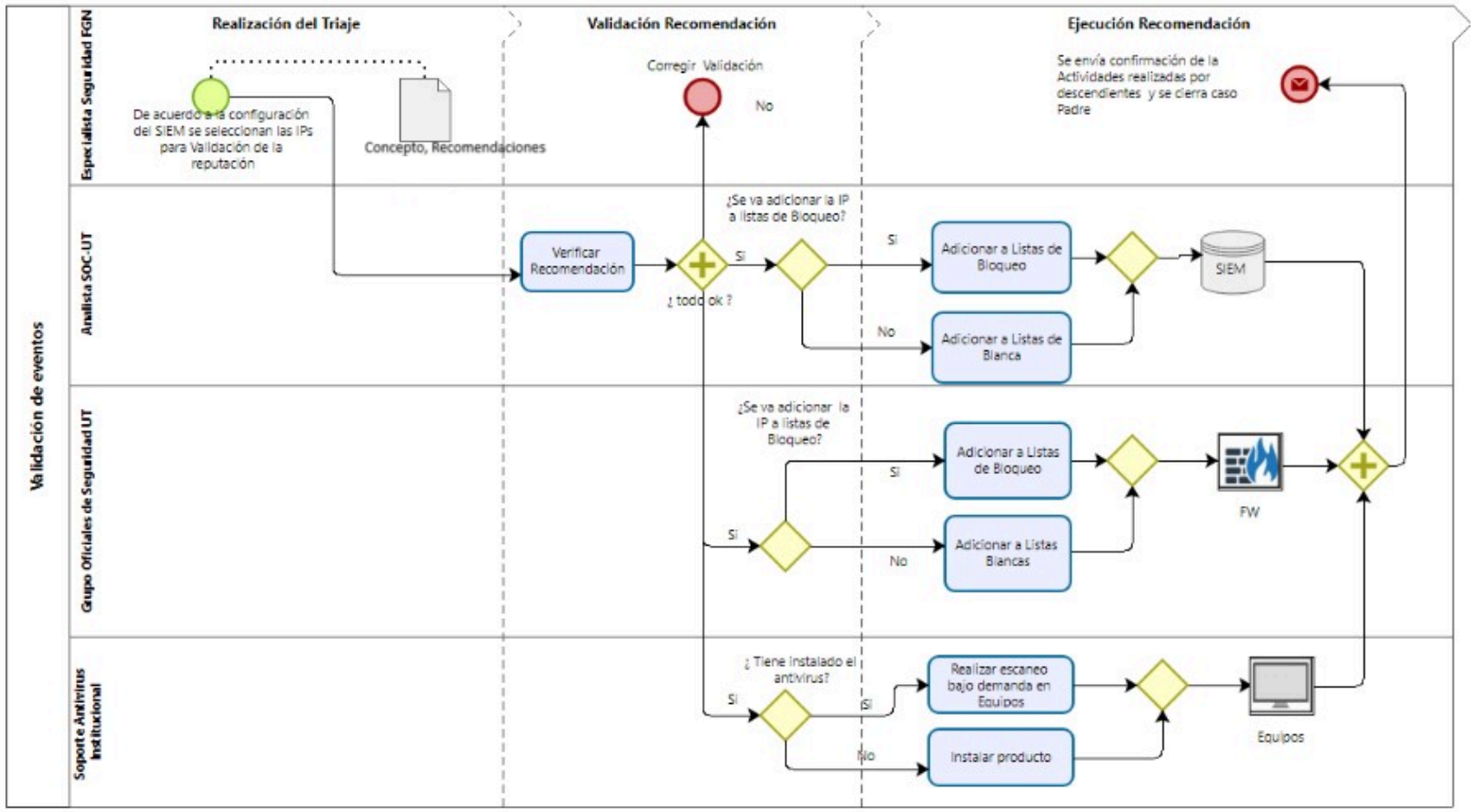
ANEXO 1. FLUJOGRAMA CREAR/MODIFICAR/ELIMINAR CASO DE USO



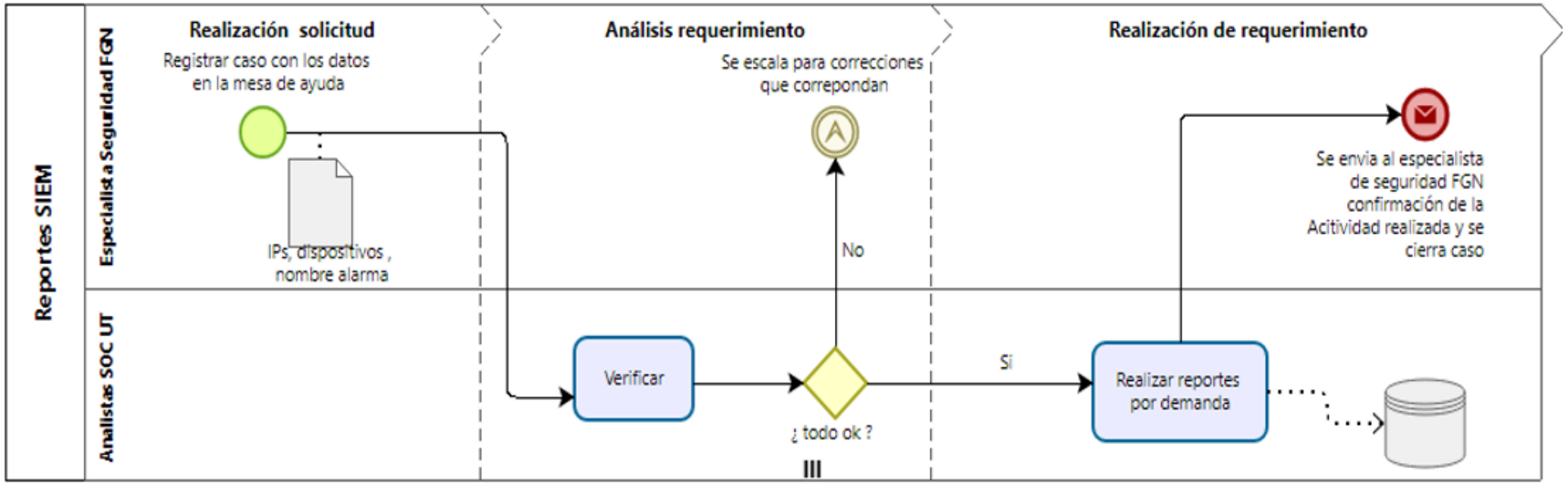
ANEXO 2. FLUJOGRAMA CREACIÓN/MODIFICACIÓN/ELIMINACIÓN DE PLAYBOOK SOAR



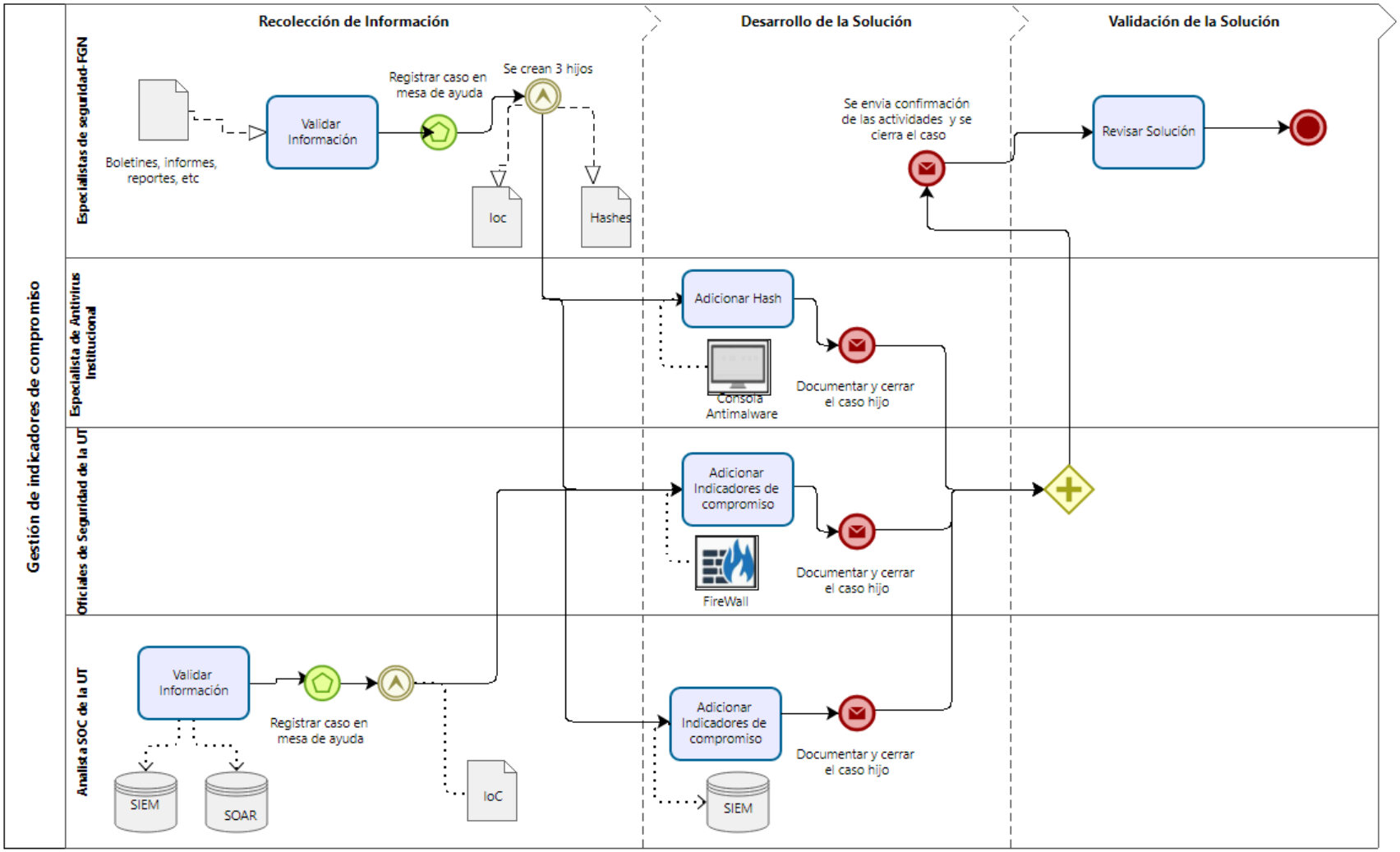
ANEXO 3. FLUJOGRAMA VALIDACIÓN DE EVENTOS



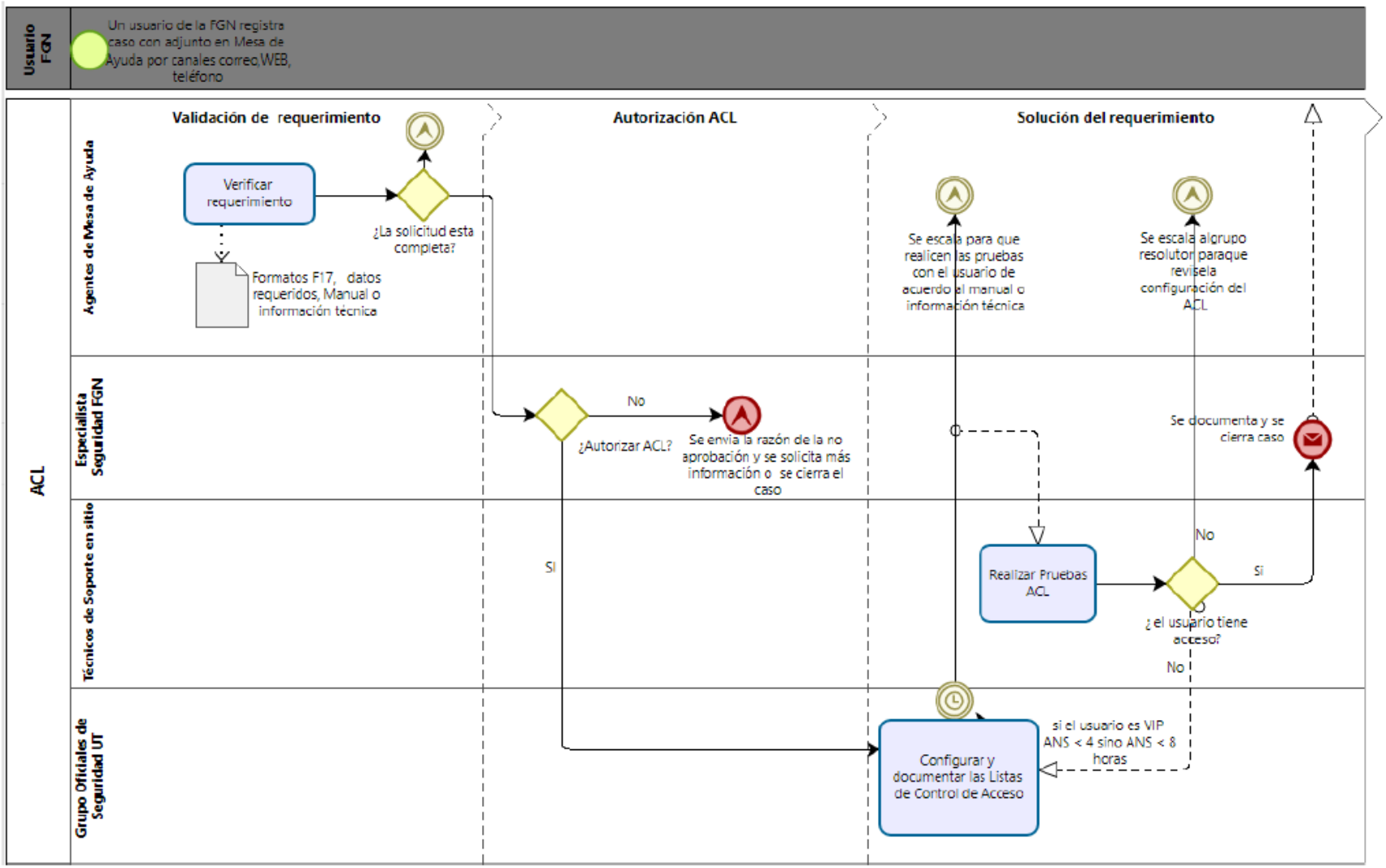
ANEXO 4. FLUJOGRAMA REPORTES SIEM



ANEXO 5. FLUJOGRAMA GESTIÓN DE INDICADORES DE COMPROMISO



ANEXO 6. FLUJOGRAMA ACL



ANEXO 7. FLUJOGRAMA CORREO, ARCHIVO O URL SOSPECHOSO