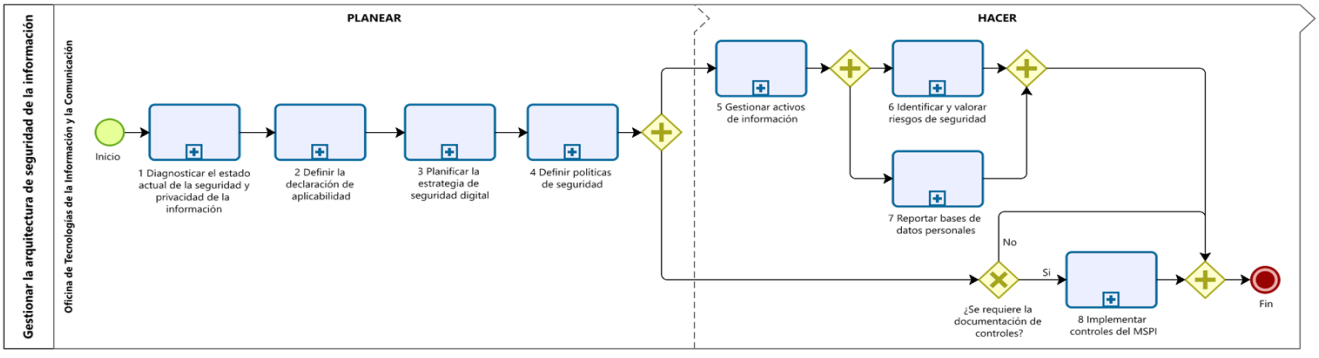
MINISTERIO DE AMBIENTE Y DESARROLLO SOSTENIBLE	**GESTIONAR LA ARQUITECTURA DE SEGURIDAD DE LA INFORMACIÓN** **Proceso:** Gestión Estratégica de Tecnologías de la Información	SOMOS IG Sistema Integrado de Gestión
Versión: 2	**Vigencia:** 03/10/2024	**Código:** P-E-GET-15

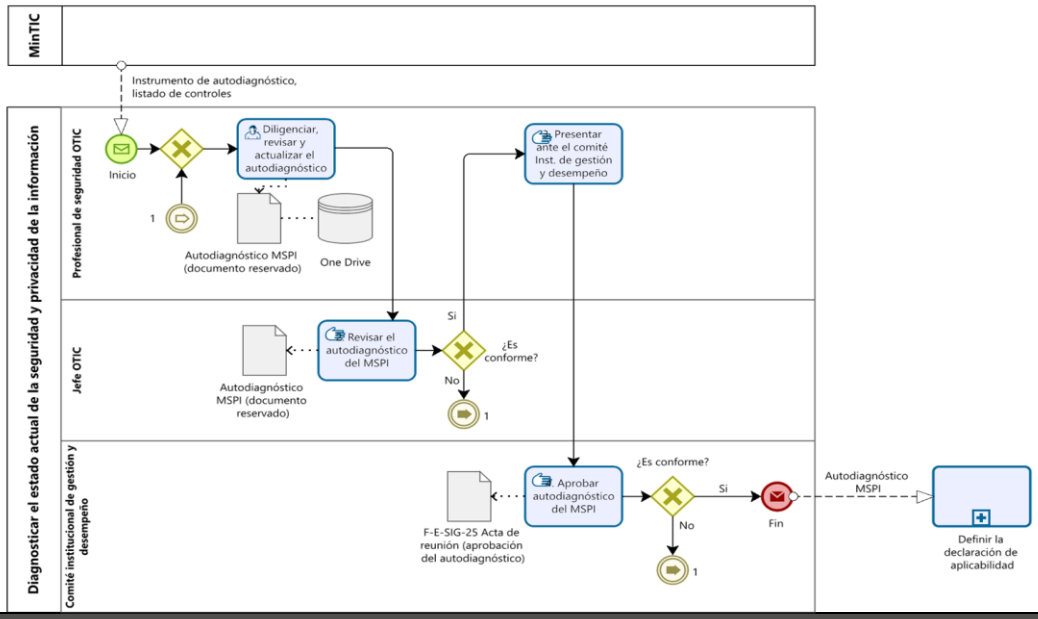
1. OBJETIVO(S)	Documentar y gestionar el Modelo de Seguridad y Privacidad de la Información, el Sistema de Gestión de Seguridad de la Información, la Arquitectura de seguridad del Marco de Referencia de Arquitectura Empresarial y demás lineamientos en términos de seguridad de la Información que deba cumplir el Ministerio de Ambiente y Desarrollo Sostenible.
2. ALCANCE	Inicia con el diagnóstico del estado actual de la seguridad y privacidad de la información pasando por definir la declaración de aplicabilidad, planificación de la estrategia de seguridad digital, definición de las políticas de seguridad, gestionar activos de información, identificar, valorar y evaluar riesgos de seguridad, reportar bases de datos personales hasta la implementación de controles de seguridad. Aplica para todas las dependencias y procesos, funcionarios, contratistas y demás partes interesadas del Ministerio de Ambiente y Desarrollo Sostenible quienes crean, procesan, transforman, comparten y almacenan información institucional o gestionan cualquier tipo de activo de información.
3.POLITICAS DE OPERACIÓN	**POLÍTICAS DE SEGURIDAD** El Comité Institucional de Gestión y Desempeño asegurará la implementación y desarrollo de las políticas de gestión y directrices en materia de seguridad digital y de la información impartidas por la Presidencia de la República y el Ministerio de Tecnologías de la Información y las Comunicaciones conforme a la resolución 2140 de 2017. **PROTECCIÓN DE ACTIVOS DE INFORMACIÓN:** La entidad, funcionarios, contratistas y terceros se comprometen a que la información clasificada como confidencial sea protegida de manera adecuada a fin de preservar su confidencialidad, integridad y disponibilidad, es así como se establecen lineamientos en la Metodología para la identificación gestión y clasificación de activos de información, y se busca generar mecanismos de protección adecuados para los activos de Información PÚBLICA – PÚBLICA CLASIFICADA – PÚBLICA RESERVADA. * El Grupo de Gestión Documental acompañará el levantamiento y consolidación de activos de información en los casos en que los líderes de proceso y los profesionales de seguridad de la OTIC lo consideren necesario conforme a las funciones definidas en la I-E-GET-02 Metodología para la identificación, gestión y clasificación de activos de información. **REPORTE BASES DE DATOS PERSONALES**: Los lideres de proceso, Jefes de Oficina y Coordinadores de Grupo, se comprometen a que anualmente deben identificar, actualizar, reportar, o solicitar la eliminación de las bases de datos personales que ya no se requieran en sus áreas, las cuales la OTIC centraliza, carga y registra en la Plataforma de la SIC en los tiempos de establecidos para esta actividad. **DECLARACIÓN DE APLICABILIDAD:** Se debe elaborar y actualizar el instrumento denominado declaración de aplicabilidad (SOA) el cual determina los controles implementados y no implementados. El instrumento debe ser aceptado y aprobado por la jefatura de la OTIC. **GESTIÓN DE RIESGOS DE SEGURIDAD Y PRIVACIDAD:** El Ministerio debe establecer la gestión de riesgos con los lineamientos establecidos por la Guía para la administración del riesgo y el diseño de controles en entidades públicas en su versión vigente, junto al Anexo Técnico referente al Modelo Nacional de Riesgos de Seguridad de la Información en las Entidades Públicas, y sus actualizaciones periódicas; así como el plan de tratamientos de riesgos. Se debe asegurar la identificación, valoración y evaluación de los riesgos que causen pérdida de confidencialidad, integridad, disponibilidad y privacidad de la información, que pueda afectar la continuidad de las operaciones. El Acuerdo de Nivel de Servicio del Grupo de comunicaciones para la publicación de documentos en sede electrónica es de 3 días hábiles.
4. NORMAS Y DOCUMENTOS DE REFERENCIA	NTC- ISO: 27001:2013. Sistemas de Gestión de Seguridad de la Información. Norma Técnica Colombiana NTC- ISO: 27002:2015. Código de prácticas para Controles de Seguridad de la Información. CONPES 3854 de 2016. Política Nacional de Seguridad digital. MRAE.DM Documento Maestro Marco de Referencia de Arquitectura Empresarial Documento Maestro del Modelo de Seguridad y Privacidad de la Información Guía para la administración del riesgo y el diseño de controles en entidades públicas del Departamento Administrativo Función Pública Resolución 2140 de 2017 del Ministerio de Ambiente y Desarrollo Sostenible 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

5. PROCEDIMIENTO

5. FLUJOGRAMA "GESTIONAR LA ARQUITECTURA DE SEGURIDAD DE LA INFORMACIÓN"



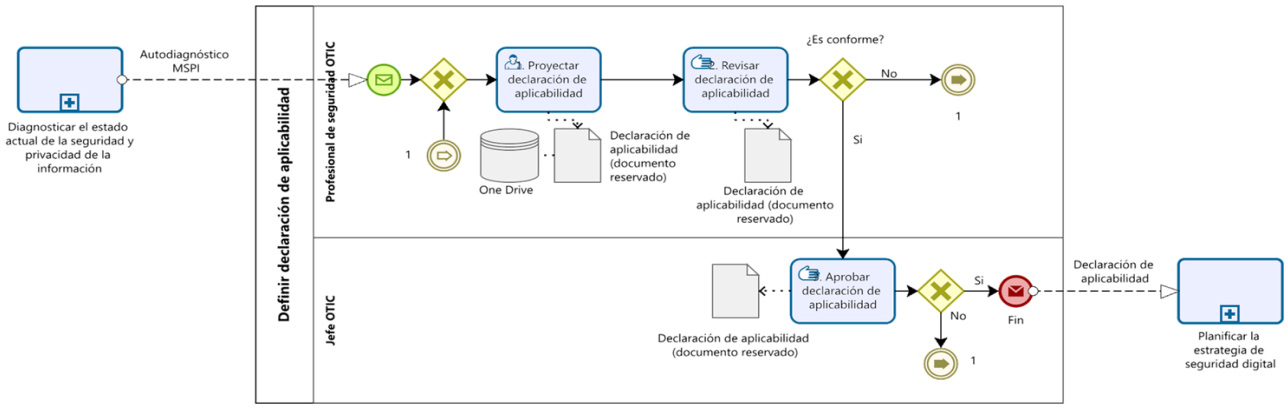
5.1.1. FLUJOGRAMA "DIAGNOSTICAR EL ESTADO ACTUAL DE LA SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN "



5.1.2. ACTIVIDADES "DIAGNOSTICAR EL ESTADO ACTUAL DE LA SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN"

N.º.	ACTIVIDAD	CICLO PHVA	DESCRIPCIÓN	RESPONSABLE	PC	REGISTRO
1	Diligenciar, revisar y actualizar el autodiagnóstico	**H**	Diligenciar, revisar y actualizar el instrumento de Autodiagnóstico del MSPI de acuerdo a los lineamientos del Ministerio TIC (Información de la entidad, listado de controles técnicos, administrativos, identificación de brechas y recomendaciones PHVA)	Profesional de Seguridad OTIC		Documento Autodiagnóstico MSPI **Diligenciado** - OneDrive
2	Revisar el autodiagnóstico del MSPI	**V**	Revisar el instrumento del autodiagnóstico del MSPI. ¿Es conforme? **Si,** Continuar con la actividad 3 "Presentar ante el Comité Institucional de Gestión y Desempeño" **No,** Continuar con la actividad 1 "Diligenciar, revisar y actualizar el autodiagnóstico".	Jefe OTIC		Documento Autodiagnóstico MSPI - **Revisado**
3	Presentar ante el Comité Institucional de Gestión y Desempeño	**H**	Presentar el documento de Autodiagnóstico MSPI ante el Comité Institucional de Gestión y Desempeño.	Profesional de Seguridad OTIC		
4	Aprobar Autodiagnóstico del MSPI	**V**	Revisar y aprobar el documento autodiagnóstico MSPI. ¿Es conforme? **Si,** Fin de la etapa. Documento Autodiagnóstico MSPI (Documento reservado) aprobado, continua la siguiente etapa de "Definir la declaración de aplicabilidad". **No,** Continuar con la actividad 1 "Diligenciar, revisar y actualizar el autodiagnóstico". **Nota:** Esta acción se realiza cuantas veces sea necesario hasta lograr la aprobación.	Comité Institucional de Gestión y Desempeño	**X**	F-E-SIG-25 Acta de reunión - **Aprobado o rechazado**

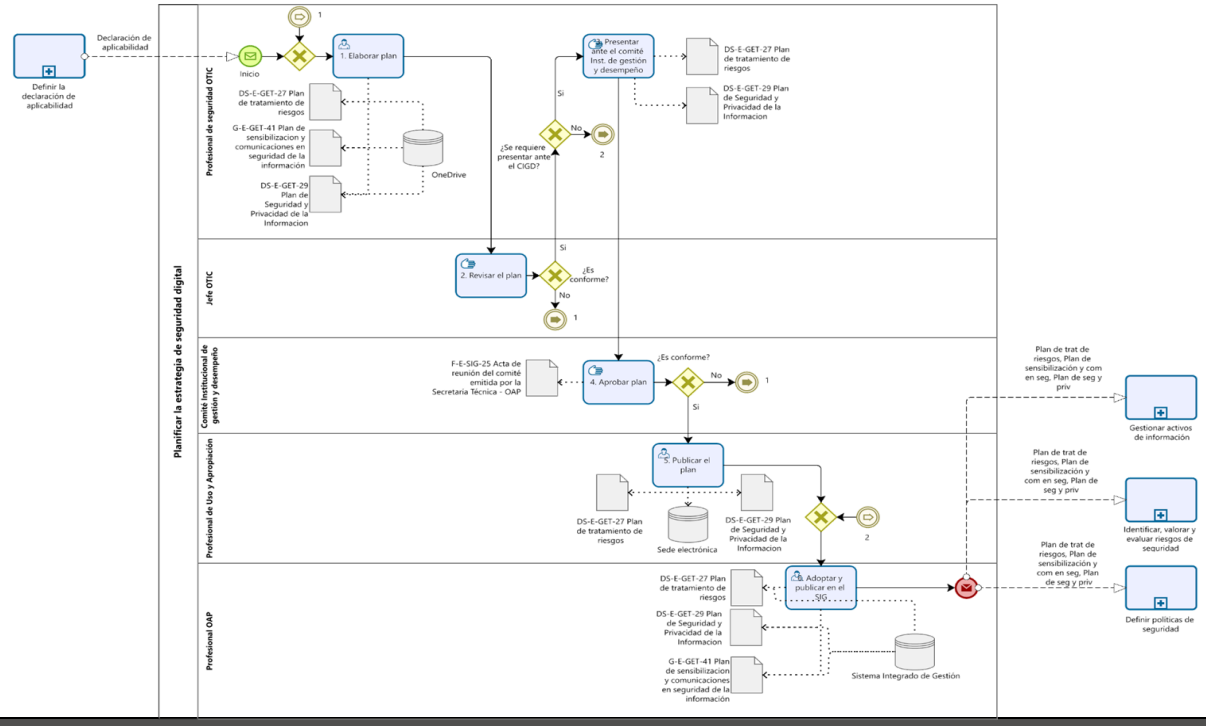
5.2.1. FLUJOGRAMA "DEFINIR DECLARACIÓN DE APLICABILIDAD"



5.2.2. ACTIVIDADES "DEFINIR DECLARACIÓN DE APLICABILIDAD"

N.º.	ACTIVIDAD	CICLO PHVA	DESCRIPCIÓN	RESPONSABLE	PC	REGISTRO
1	Proyectar declaración de aplicabilidad	**H**	Proyectar la declaración de aplicabilidad con las justificaciones de la aplicación de los controles, así como la justificación de las exclusiones. Una vez terminado el documento precederá a enviar vía correo electrónico al Responsable de seguridad OTIC.	Profesional de Seguridad OTIC		Documento Declaración de aplicabilidad- **Elaborado** en el OneDrive
2	Revisar declaración de aplicabilidad	**V**	El Profesional de Seguridad OTIC **(o su delegado)** debe Revisar el documento de Declaración de Aplicabilidad de acuerdo con los controles identificados. ¿Es conforme? **Si,** Continuar con la actividad 3 "Aprobar declaración de aplicabilidad" **No,** Continuar con la actividad 1 "Proyectar declaración de aplicabilidad". **Nota:** Si el documento está conforme, el Responsable de Seguridad OTIC es el responsable de enviar vía correo electrónico el documento Declaración de Aplicabilidad al Jefe OTIC.	Profesional de Seguridad OTIC (o su delegado)		Documento Declaración de aplicabilidad - **Revisado**
3	Aprobar declaración de aplicabilidad	**A**	Aprobar la Declaración de aplicabilidad. ¿Es conforme? **Si,** Fin de la etapa. Continua con la siguiente etapa de "Planificar la estrategia de seguridad digital" **No,** Continuar con la actividad 1 "Proyectar declaración de aplicabilidad". **Nota:** Esta acción se realiza cuantas veces sea necesario hasta lograr la aprobación.	Jefe OTIC	**X**	Declaración de aplicabilidad (documento reservado) - **Aprobado o rechazado**

5.3.1. FLUJOGRAMA "PLANIFICAR LA ESTRATEGIA DE SEGURIDAD DIGITAL"

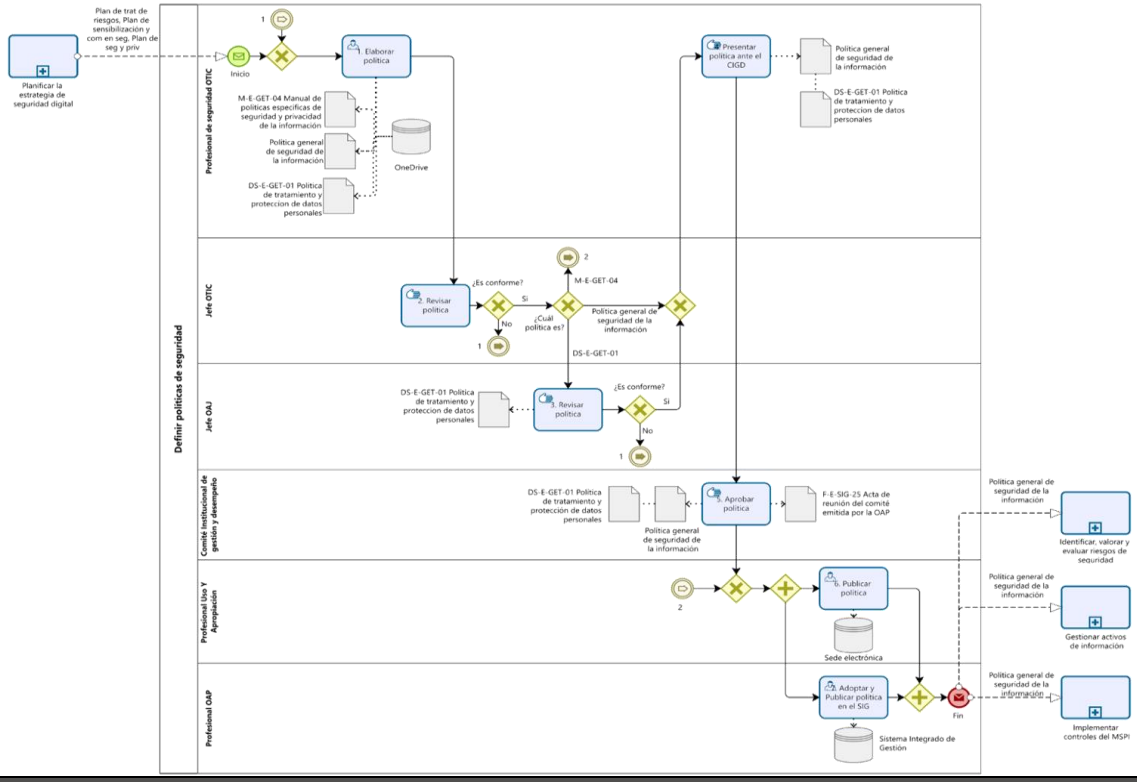


5.3.2. ACTIVIDADES "PLANIFICAR LA ESTRATEGIA DE SEGURIDAD DIGITAL"

N.º.	ACTIVIDAD	CICLO PHVA	DESCRIPCIÓN	RESPONSABLE	PC	REGISTRO
1	Elaborar plan	**H**	El Profesional de Seguridad OTIC debe elaborar: Plan de Tratamiento de Riesgos Plan de Seguridad y Privacidad de la Información y/o el Plan de Sensibilización y Comunicaciones en Seguridad de la Información.	Profesional de Seguridad OTIC		Documentos (DS-E-GET-27 Plan de tratamiento de Riesgos, DS-E-GET-29 Plan de Seguridad y Privacidad de la Información y/o G-E-GET-41 Plan de Sensibilización y Comunicaciones en Seguridad de la Información) - **Elaborado(s)** OneDrive
2	Revisar el plan	**V**	Revisar el plan (Plan de Tratamiento de Riesgos, el Plan de Sensibilización y Comunicaciones en Seguridad de la Información y el Plan de Seguridad y Privacidad de la Información) y dar su Vo. Bo. de conformidad. ¿Es conforme? **No,** Continuar con la actividad 1 "Elaborar plan" **Si,** Continuar con la siguiente pregunta ¿Se requiere presentar ante el GIGD (Comité Institucional de Gestión y Desempeño)? **Si,** Continuar con actividad 3 "Presentar ante el Comité de Gestión y Desempeño" **No,** Continuar con actividad 6 "Adoptar y publicar en el SIG"	Jefe OTIC	**X**	Documentos (DS-E-GET-27 Plan de tratamiento de Riesgos, DS-E-GET-29 Plan de Seguridad y Privacidad de la Información y/o G-E-GET-41 Plan de Sensibilización y Comunicaciones en Seguridad de la Información) - **Revisado(s)**
3	Presentar ante el Comité Institucional de Gestión y Desempeño	**H**	El Profesional de Seguridad OTIC de acuerdo a los requerimientos del Comité de Gestión y Desempeño, deberá realizar presentación y entrega del **DS-E-GET-27** Plan de Tratamiento de Riesgos y el **DS-E-GET-29** Plan de Seguridad y Privacidad de la Información los cuáles se someterán a aprobación.	Profesional de Seguridad OTIC		
4	Aprobar plan	**V**	Revisar y aprobar los planes (**DS-E-GET-27** Plan de Tratamiento de Riesgos y el **DS-E-GET-29** Plan de Seguridad y Privacidad de la Información). ¿Es conforme? **Si,** Continuar con actividad 5 "Publicar el plan" **No,** Continuar con la actividad 1 "Elaborar plan ".	Comité de Gestión y Desempeño	**X**	Documento F-E-SIG-25 Acta de reunión - **Aprobado o rechazado**

5	Publicar el plan	**A**	Profesional de Uso y Apropiación deberá solicitar al Profesional Grupo de Comunicaciones vía correo electrónico publicar el plan (Plan de Tratamiento de Riesgos y el Plan de Seguridad y Privacidad de la Información) en sede electrónica.	Profesional de Uso y Apropiación	**X**	Documentos (DS-E-GET-27 Plan de Tratamiento de Riesgos y DS-E-GET-29 Plan de Seguridad y Privacidad de la Información) - **Publicados** en sede electrónica
6	Adoptar y publicar en el SIG	**A**	Actualizar los planes en el Sistema Integrado de Gestión. Fin de la etapa. Continua con la siguiente etapa "Definir políticas de seguridad".	Profesional Oficina Asesora Planeación OAP	**X**	Documentos (DS-E-GET-27 Plan de tratamiento de Riesgos, DS-E-GET-29 Plan de Seguridad y Privacidad de la Información y/o G-E-GET-41 Plan de Sensibilización y Comunicaciones en Seguridad de la Información) - **Actualizados** en el Sistema Integrado de Gestión

5.4.1. FLUJOGRAMA "DEFINIR POLÍTICAS DE SEGURIDAD"

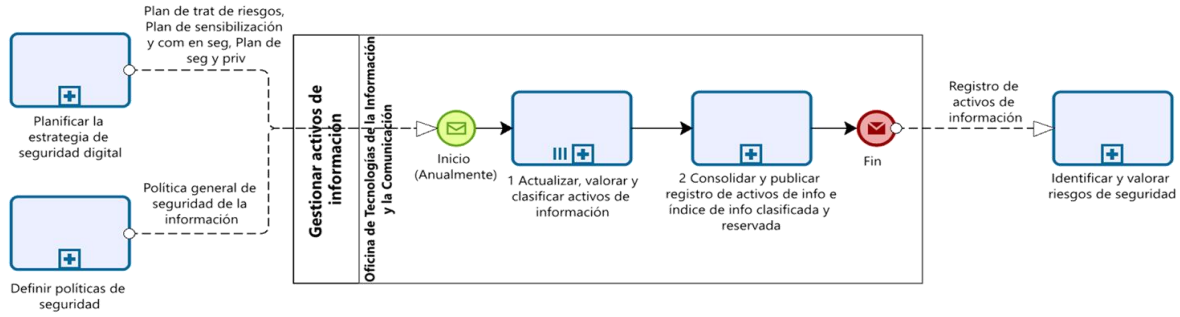


5.4.2. ACTIVIDADES "DEFINIR POLÍTICAS DE SEGURIDAD"

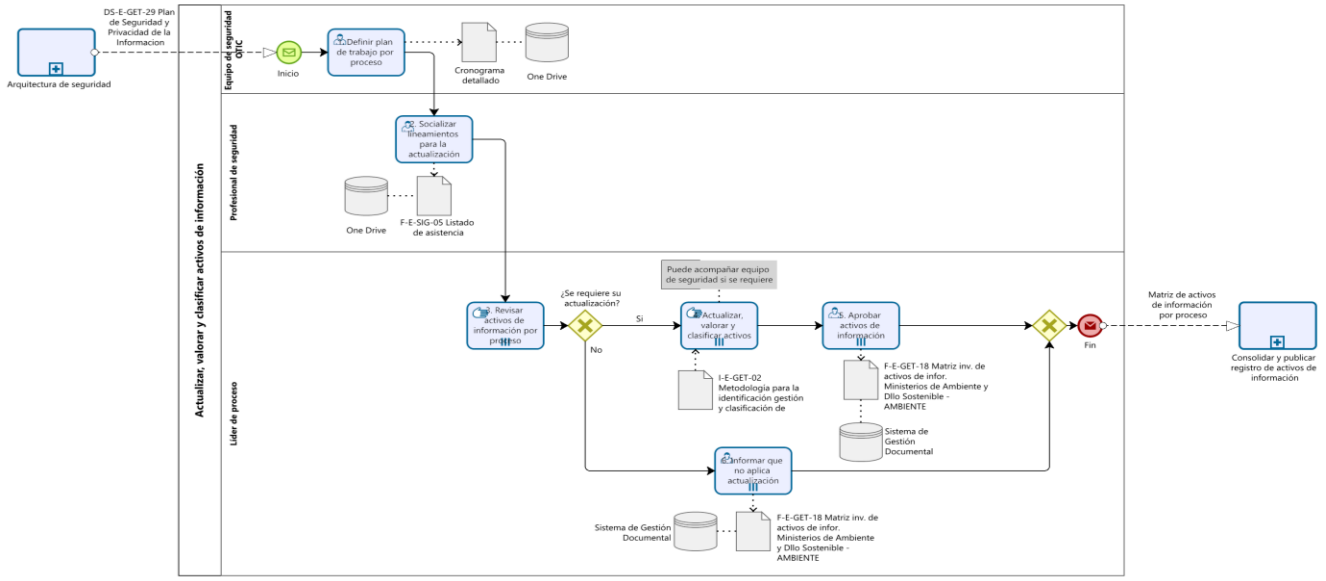
N.º.	ACTIVIDAD	CICLO PHVA	DESCRIPCIÓN	RESPONSABLE	PC	REGISTRO
1	Elaborar política	**H**	Elaborar o actualizar la política (Política general de seguridad de la información, **DS-E-GET-01** Política de tratamiento y protección de datos personales y/o **M-E-GET-04** Manual de políticas específicas de seguridad y privacidad de la información. El **M-E-GET-04** se debe revisar anualmente, y determinar si requiere actualización. El **M-E-GET-04** y **DS-E-GET-01** se pueden proyectar y actualizar cuando se requiera de manera independiente.	Profesional de Seguridad OTIC		Documentos (Política general de seguridad de la información y/o M-E-GET-04 Manual de políticas específicas de seguridad de la información y/o DS-E-GET-01 Política de tratamiento y protección de datos personales) - **Elaborados o Actualizados** en el OneDrive

2	Revisar política	**V**	Revisar la Política. ¿Es conforme? **No,** Continuar con la actividad 1 "Elaborar política". **Si,** ¿Cuál política es? **DS-E-GET-01,** Continuar con actividad 3 "Revisar política" **Política general de seguridad de la información,** Continuar con actividad 4 "Presentar política ante Comité Institucional de Gestión y Desempeño". **M-E-GET-04,** Continuar con actividad 6 "Publicar política" y 7 "Adoptar y Publicar política en el SIG" de manera paralela. **Nota:** Una vez revisada la **DS-E-GET-01** Política de Tratamiento y Protección de Datos Personales, el Profesional de Seguridad OTIC es el responsable de enviarla a la oficina Asesora Jurídica a través del Sistema de Gestión Documental	Jefe OTIC	**X**	Documentos (Política general de seguridad de la información y/o M-E-GET-04 Manual de políticas específicas de seguridad de la información y/o DS-E-GET-01 Política de tratamiento y protección de datos personales) - **Revisados**
3	Revisar política	**V**	Revisar de manera integral la **DS-E-GET-01** Política de tratamiento y protección de datos personales. ¿Es conforme? **Si,** Continuar con actividad 4 "Presentar política ante Comité de Gestión y Desempeño" **No,** Continuar con actividad 1 "Elaborar política".	Jefe Oficina Asesora Jurídica		Documento DS-E-GET-01 Política de tratamiento y protección de datos personales - **Revisada** y enviada a través del Sistema de Gestión Documental
4	Presentar política ante Comité Institucional de Gestión y Desempeño	**H**	Presentar la Política general de seguridad de la información y/o **DS-E-GET-01** Política de Tratamiento y Protección de Datos Personales ante el Comité Institucional de Gestión y Desempeño para su aprobación.	Profesional de Seguridad OTIC		
5	Aprobar política	**V**	Revisar y aprobar la Política general de seguridad de la información y/o **DS-E-GET-01** Política de tratamiento y protección de datos personales. Continuar con actividades 6 y 7 de manera paralela.	Comité de Gestión y Desempeño	**X**	Documento F-E-SIG-25 Acta de reunión - **Aprobado o rechazado**
6	Publicar política	**A**	Solicitar al Profesional del Grupo de Comunicaciones publicar la política aprobada en la sede electrónica. Fin de la etapa.	Profesional de Uso y Apropiación	**X**	Documentos (Política general de seguridad de la información y/o M-E-GET-04 Manual de políticas específicas de seguridad de la información y/o DS-E-GET-01 Política de tratamiento y protección de datos personales) - **Publicados** en sede electrónica
7	Adoptar y Publicar política en el SIG	**A**	Publicar o actualizar la política aprobada en el Sistema Integrado de Gestión. Fin de la etapa.	Profesional Oficina Asesora de Planeación - OAP	**X**	Política general de seguridad de la información y/o M-E-GET-04 Manual de políticas específicas de seguridad de la información y/o DS-E-GET-01 Política de tratamiento y protección de datos personales - **Publicados o actualizados** en el Sistema Integrado de Gestión

5.5.1. FLUJOGRAMA "GESTIONAR ACTIVOS DE INFORMACIÓN"



5.5.1.1 FLUJOGRAMA "ACTUALIZAR,VALORAR Y CLASIFICAR ACTIVOS DE INFORMACIÓN"

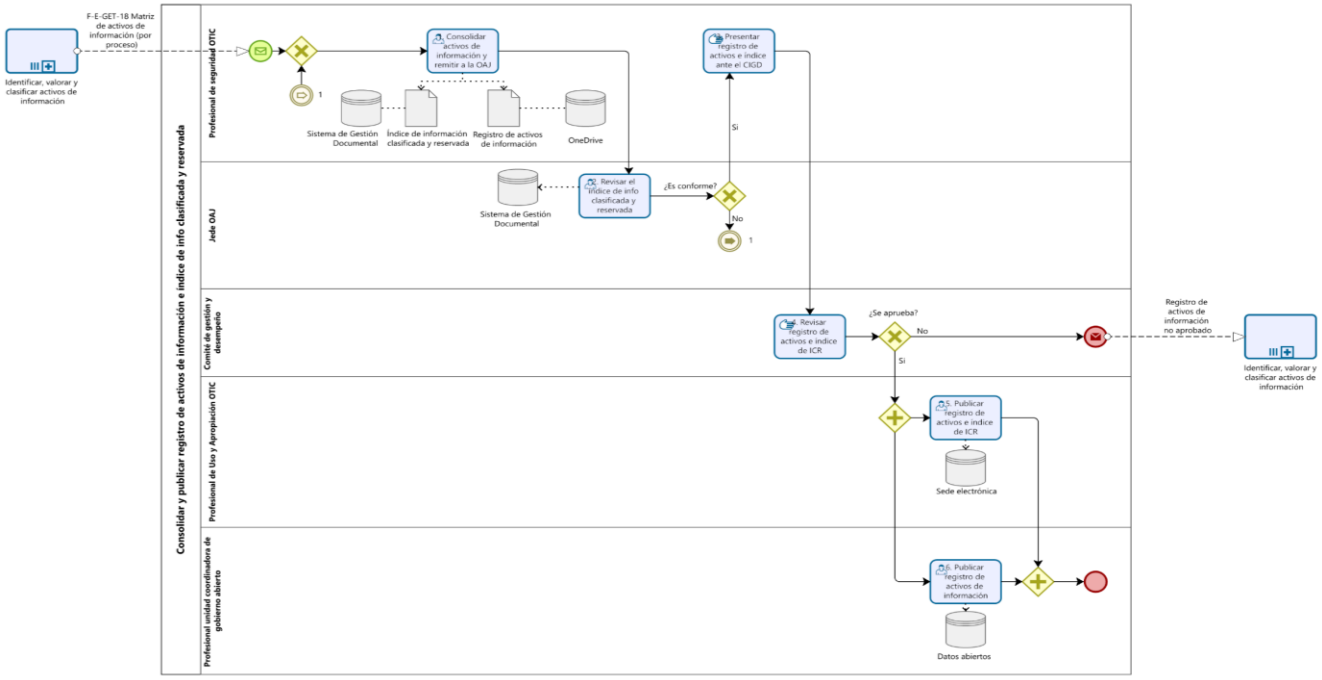


5.5.1.2 ACTIVIDADES "ACTUALIZAR,VALORAR Y CLASIFICAR ACTIVOS DE INFORMACIÓN"

N.º.	ACTIVIDAD	CICLO PHVA	DESCRIPCIÓN	RESPONSABLE	PC	REGISTRO
1	Definir plan de trabajo por proceso	P	En mesa de trabajo se debe Determinar las actividades proyectadas con el tiempo estimado para la actualización de activos de información en un cronograma de trabajo.	Equipo de Seguridad OTIC	X	Documento Cronograma de trabajo - **Elaborado** OneDrive
2	Socializar lineamientos para la actualización	H	Profesional de Seguridad **(o su delegado)** debe socializar los lineamientos para la actualización de los activos de información a los líderes de proceso y/o sus delegados.	Profesional de Seguridad (o su delegado)	X	Documento F-E-SIG-05 Listado de asistencia en el sistema de gestión documental o grabación o listado de asistencia Teams o correo electrónico o pieza comunicativa en el OneDrive
3	Revisar activos de información por proceso	H	Revisar el documento **F-E-GET-18** Matriz inventario de activos de información Ministerio de Ambiente y Desarrollo Sostenible - AMBIENTE vigente con el objetivo de determinar si un activo de información continua o no siendo parte de su inventario o si la clasificación, valoración u otro tipo de atributo que hace parte de la matriz debe ser modificado o actualizado conforme al **I-E-GET-02** Metodología para la identificación, gestión y clasificación de activos de información ¿Se requiere su actualización? **Si,** Continuar con actividad 4 "Actualizar, valorar y clasificar activos" **No,** Continuar con actividad 6 "Informar que no aplica actualización por el Sistema de Gestión Documental"	Líder de Proceso		
4	Actualizar, valorar y clasificar activos	H	Actualizar, valorar y clasificar los activos de información diligenciando el formato **F-E-GET-18** Matriz inventario de activos de información Ministerio de Ambiente y Desarrollo Sostenible - AMBIENTE, conforme al instructivo **I-E-GET-02** Metodología para la identificación, gestión y clasificación de activos de información **Nota:** Se puede solicitar acompañamiento del Equipo de Seguridad si se requiere.	Líder de Proceso		

5	Aprobar activos de información	**H**	Remitir oficialmente mediante memorando al Responsable de Seguridad, la aprobación de la actualización de su inventario de activos de información, adjuntando la Matriz Inventario de Activos de Información diligenciada en el formato establecido. Fin de la etapa. Continua con la siguiente etapa "Consolidar y publicar registro de activos de información".	Líder de Proceso	**X**	Memorando oficial de aprobación del inventario de activos de información y el documento F-E-GET-18 Matriz inventario de activos de información Ministerio de Ambiente y Desarrollo Sostenible – AMBIENTE **Actualizado** - **Radicados** en el sistema de gestión documental.
6	Informar que no aplica actualización	**H**	Remitir oficialmente mediante memorando al responsable de seguridad, indicando que no aplica la actualización de los activos de información del proceso que lidera; adjuntando al **F-E-GET-18** Matriz inventario de activos de información Ministerio de Ambiente y Desarrollo Sostenible – AMBIENTE vigente. Fin de la etapa. Continua con la siguiente etapa "Consolidar y publicar registro de activos de información".	Líder de Proceso	**X**	Memorando oficial de aprobación del inventario de activos de información y el F-E-GET-18 Matriz inventario de activos de información Ministerio de Ambiente y Desarrollo Sostenible – AMBIENTE vigente - **Radicados** en el sistema de gestión documental.

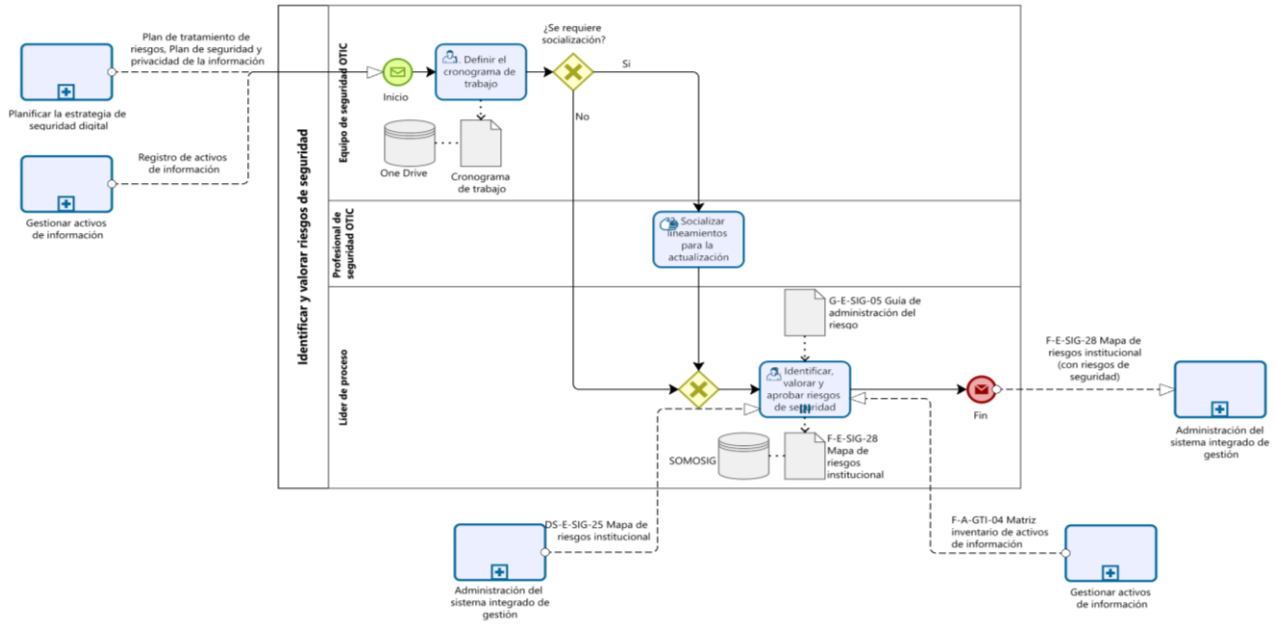
5.5.2.1 FLUJOGRAMA "CONSOLIDAR Y PUBLICAR REGISTRO DE ACTIVOS DE INFORMACIÓN E ÍNDICE DE INFORMACIÓN CLASIFICADA Y RESERVADA"



5.5.2.2 ACTIVIDADES "CONSOLIDAR Y PUBLICAR REGISTRO DE ACTIVOS DE INFORMACIÓN E ÍNDICE DE INFORMACIÓN CLASIFICADA Y RESERVADA"

N.º.	ACTIVIDAD	CICLO PHVA	DESCRIPCIÓN	RESPONSABLE	PC	REGISTRO
1	Consolidar activos de información y remitir a la Oficina Asesora Jurídica	H	Profesional de Seguridad OTIC una vez recibida la aprobación del inventario de activos de información por parte del líder de cada proceso o dependencia, consolida la información en el formato **F-E-GET-18** Matriz inventario de activos de información Ministerio de Ambiente y Desarrollo Sostenible - AMBIENTE para generar el registro de activos de información y el Índice de Información Clasificada y Reservada, de acuerdo a los lineamientos establecidos. Posteriormente, debe remitir a través del Sistema de Gestión Documental la Información Clasificada y Reservada para revisión por parte de la Oficina Asesora Jurídica.	Profesional de Seguridad OTIC		Registro de Activos de Información **Actualizado** - OneDrive Índice de Información Clasificada y Reservada - **Radicado** en sistema de gestión documental
2	Revisar el índice de información clasificada y reservada	V	Revisar el índice de información clasificada y reservada radicado en el sistema de gestión documental y emitir su visto bueno o comentarios mediante memorando por el mismo medio. ¿Es conforme? **Si,** Continuar con actividad 3 "Presentar registro de activos e índice ante el Comité Institucional de Gestión y Desempeño". **No,** Continuar con actividad 1 "Consolidar activos de información y remitir a la Oficina Asesora Jurídica"	Jefe Oficina Asesora Jurídica	X	Índice de Información Clasificada y Reservada - **Revisado y radicado** mediante sistema de gestión documental.
3	Presentar registro de activos e índice ante el CIGD Comité Institucional de Gestión y Desempeño	H	Profesional de Seguridad OTIC **o su delegado** Presentar el registro de activos de información y el índice de información clasificada y reservada ante el Comité Institucional de Gestión y Desempeño para su respectiva aprobación.	Profesional de Seguridad OTIC (o su delegado)		
4	Revisar y aprobar el registro de activos e Índice de Información clasificada y reservada	V	Revisar y aprobar el Índice de Información Clasificada y Reservada y el Registro de Activos de Información. ¿Se aprueba? **Si,** Continuar con la actividad 5 "Publicar registro de activos e Índice de Información Clasificada y Reservada" y 6 "Publicar registro de activos de información" de manera paralela. **No,** Continuar con la actividad 1 de la etapa Identificar, valorar y clasificar activos de información.	Comité de Gestión y Desempeño	X	Documento F-E-SIG-25 Acta de reunión - **Aprobado o rechazado**
5	Publicar registro de activos e Índice de Información Clasificada y Reservada	A	Solicitar al Profesional del Grupo de Comunicaciones, la publicación del índice de Información Clasificada y Reservada y el Registro de Activos de Información en sede electrónica. **Nota:** El Grupo de comunicaciones publica los documentos consolidados en el mismo formato enviado por el Responsable de seguridad.	Profesional de Uso y Apropiación	X	Documentos (Matrices del Índice de Información Clasificada y Reservada y Registro de Activos de Información) - **Publicados** en la sede electrónica del Ministerio
6	Publicar registro de activos de información	A	El Responsable de seguridad de la entidad debe solicitar la publicación del Registro de Activos de Información en el portal de datos abiertos al profesional de la Unidad Coordinadora de Gobierno Abierto. El Profesional de la Unidad de Gobierno Abierto debe publicar el registro de activos de información en el portal de datos abiertos. Fin de la etapa.	Profesional Unidad Coordinadora de Gobierno Abierto	X	Registro de Activos de Información - **Publicado** en el portal de datos abiertos

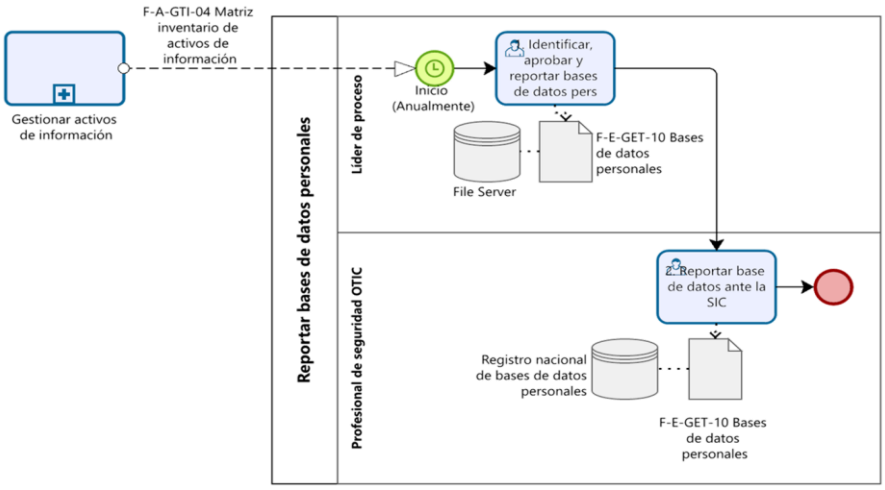
5.6.1. FLUJOGRAMA "IDENTIFICAR Y VALORAR RIESGOS DE SEGURIDAD"



5.6.2. ACTIVIDADES "IDENTIFICAR Y VALORAR RIESGOS DE SEGURIDAD"

N.º.	ACTIVIDAD	CICLO PHVA	DESCRIPCIÓN	RESPONSABLE	PC	REGISTRO
1	Definir el cronograma de trabajo	P	En mesa de trabajo se debe determinar las actividades necesarias para la identificación y valoración de riesgos. ¿Se requiere socialización? **Si**, Continuar con actividad 2 "Socializar lineamientos para la actualización". **No**, Continuar con actividad 3 "Identificar, valorar y aprobar riesgos de seguridad".	Equipo de Seguridad OTIC		Cronograma de trabajo **elaborado -** OneDrive
2	Socializar lineamientos para la actualización	H	El Profesional de Seguridad OTIC **o su delegado** socializar lineamientos sobre los riesgos de seguridad a los líderes de proceso.	Profesional de Seguridad OTIC (o su delegado)		
3	Identificar, valorar y aprobar riesgos de seguridad	H	Identificar, valorar y aprobar riesgos de seguridad conforme a la **G-E-SIG-05** Guía de administración del riesgo.	Líder de Proceso	**X**	**F-E-SIG-28** Mapa de riesgos institucional (con riesgos de seguridad) **actualizados** en aplicativo SOMOSIG

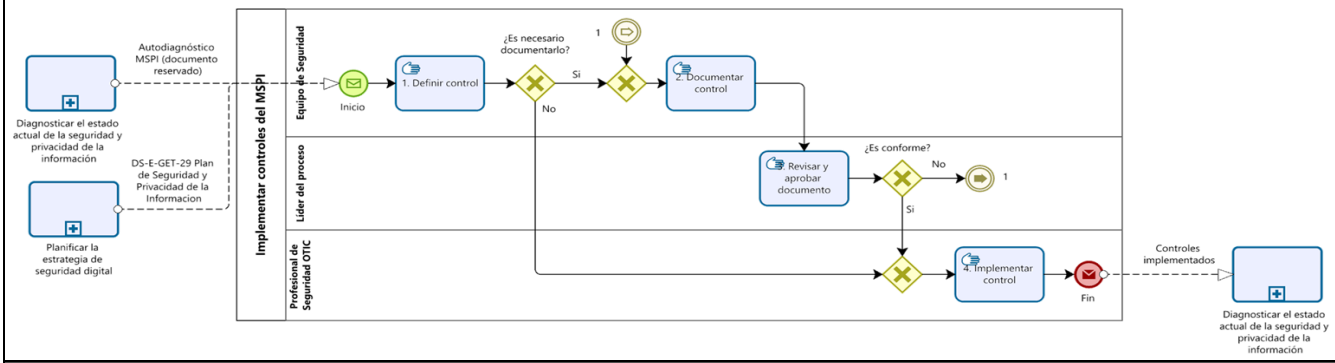
5.7.1. FLUJOGRAMA "REPORTAR BASES DE DATOS PERSONALES "



5.7.2. ACTIVIDADES "REPORTAR BASES DE DATOS PERSONALES "

N.º.	ACTIVIDAD	CICLO PHVA	DESCRIPCIÓN	RESPONSABLE	PC	REGISTRO
1	Identificar, aprobar y reportar bases de datos personales	H	Identificar en la Matriz inventario de activos de información las bases de datos personales reportadas y consignar la información en el formato **F-E-GET-10** Reporte de bases de datos personales. Esta actividad debe realizarse anualmente.	Líder de Proceso		Documento F-E-GET-10 Reporte de bases de datos personales **actualizada** - File Server
2	Reportar Base de Datos en la SIC	A	Reportar la base de datos en el Registro nacional de bases de datos personales en la Superintendencia de Industria y Comercio - SIC . Superintendencia de Industria y Comercio - SIC emite un Certificado como constancia del reporte las bases de datos. Fin de la etapa.	Profesional de Seguridad OTIC	X	Certificado de registro de bases de datos **Emitido** en el Registro de bases de datos personales

5.8.1 FLUJOGRAMA "IMPLEMENTAR CONTROLES DEL MSPI"



5.8.2 ACTIVIDADES "IMPLEMENTAR CONTROLES DEL MSPI"

N.º.	ACTIVIDAD	CICLO PHVA	DESCRIPCIÓN	RESPONSABLE	PC	REGISTRO
1	Definir control	P	Definir el mecanismo y el delegado para implementar controles del MSPI. ¿Es necesario documentarlo? **Si,** Continuar con la actividad 2 "Documentar control" **No**, Continuar con la actividad 4 "Implementar control".	Equipo de Seguridad OTIC		
2	Documentar control	H	Documentar los controles del MSPI.	Equipo de Seguridad OTIC		Documento MSPI - **Actualizado** - OneDrive
3	Revisar y aprobar documento	V	Revisar y aprobar el documento con los controles del MSPI. ¿Es conforme? **Si,** Continuar con la actividad 4 "Implementar control" **No,** Continuar con la actividad 2 "Documentar control"	Líder de Proceso	X	Documento MSPI - **Aprobado o rechazado** - OneDrive
4	Implementar control	A	El Profesional de Seguridad OTIC **o su delegado Responsable del Control** Implementar el control de acuerdo con lo definido en el documento MSPI.	Profesional de Seguridad OTIC (o su delegado Responsable del Control)	X	Control implementado

6. TÉRMINOS Y DEFINICIONES

Activo: En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de ésta (sistemas, soportes, edificios, personas, etc.) que tenga valor para la organización. (ISO/IEC 27000).
Confidencialidad: Propiedad que determina la condición de que la información no está disponible ni sea revelada a individuos, entidades o procesos no autorizados.
Bases de Datos Personales: Conjunto organizado de datos personales que será objeto de Tratamiento (Ley 1581 de 2012, art 3)
Disponibilidad: Propiedad de que la información sea accesible y utilizable por solicitud de una entidad autorizada.
Integridad: Propiedad de salvaguardar la exactitud y estado completo de los activos.
Información Pública Clasificada: Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, pertenece al ámbito propio, particular y privado o semiprivado de una persona natural o jurídica por lo que su acceso podrá ser negado o exceptuado, siempre que se trate de las circunstancias legítimas y necesarias y los derechos particulares o privados consagrados en el artículo 18 de la Ley 1712 de 2014.
MSPI: Modelo de Seguridad y Privacidad de la Información el cual imparte lineamientos a las entidades públicas en materia de implementación y adopción de buenas prácticas, tomando como referencia estándares internacionales, con el objetivo de orientar la gestión e implementación adecuada del ciclo de vida de la seguridad de la información (Planeación, Implementación, Evaluación, Mejora Continua), permitiendo habilitar la implementación de la Política de Gobierno Digital.
Riesgo: Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias. (ISO/IEC 27000).
SIC: Superintendencia de Industria y Comercio: Autoridad nacional de protección de la competencia de los datos personales.