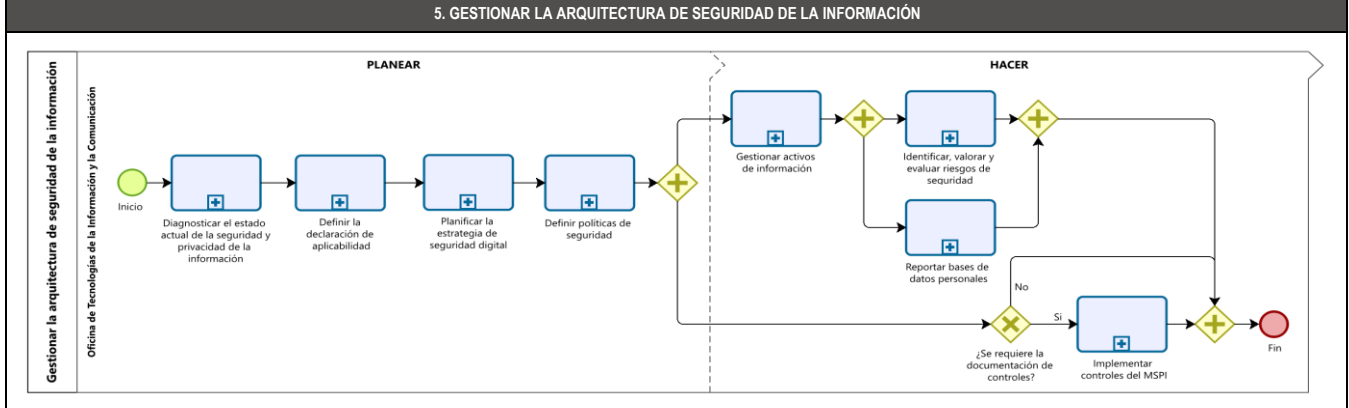


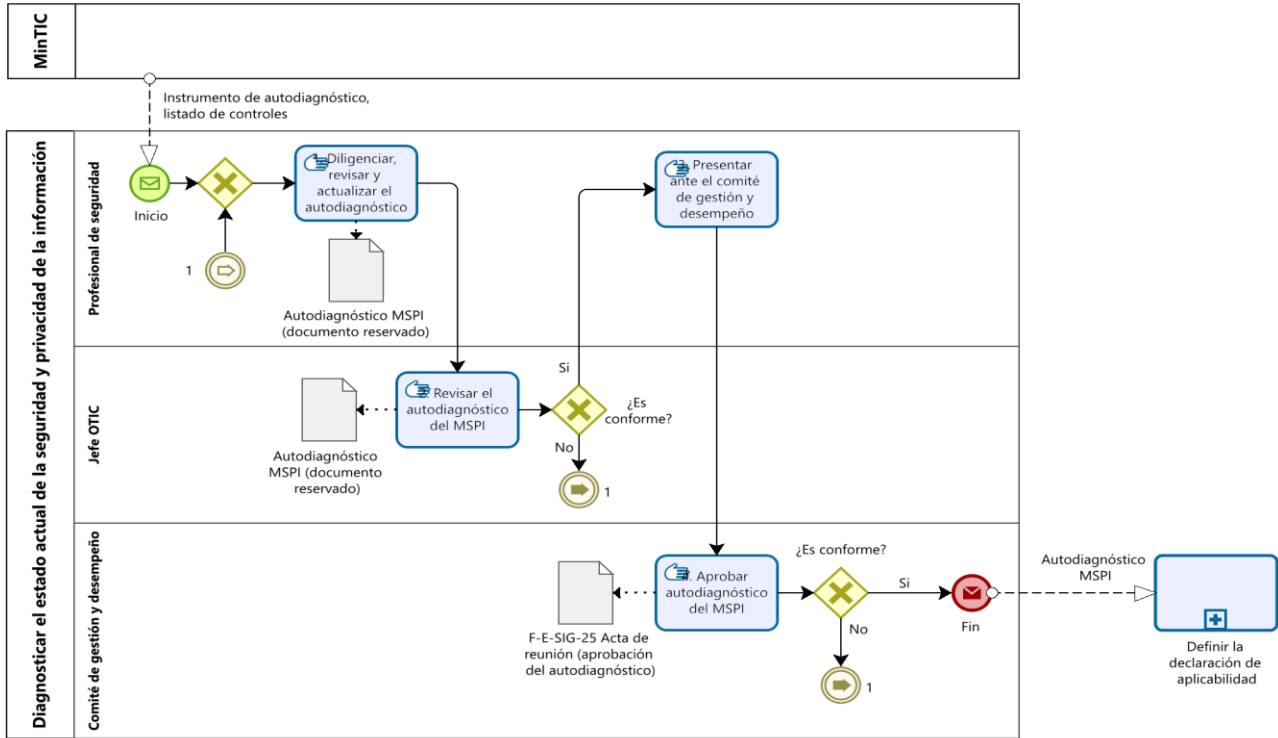
1. OBJETIVO(S)	Documentar y gestionar el Modelo de Seguridad y Privacidad de la Información, el Sistema de Gestión de Seguridad de la Información, la Arquitectura de seguridad del Marco de Referencia de Arquitectura Empresarial y demás lineamientos en términos de seguridad de la Información que deba cumplir el Ministerio de Ambiente y Desarrollo Sostenible.
2. ALCANCE	<p>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.</p> <p>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.</p>
3. POLITICAS DE OPERACIÓN	<p>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.</p> <p>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.</p> <p>* 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</p> <p>REPORTE BASES DE DATOS PERSONALES: Los líderes 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.</p> <p>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.</p> <p>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.</p> <p>El Acuerdo de Nivel de Servicio del Grupo de comunicaciones para la publicación de documentos en sede electrónica es de 3 días hábiles.</p>
4. NORMAS Y DOCUMENTOS DE REFERENCIA	<p>NTC- ISO: 27001:2013. Sistemas de Gestión de Seguridad de la Información. Norma Técnica Colombiana</p> <p>NTC- ISO: 27002:2015. Código de prácticas para Controles de Seguridad de la Información.</p> <p>CONPES 3854 de 2016. Política Nacional de Seguridad digital.</p> <p>MRAE.DM Documento Maestro Marco de Referencia de Arquitectura Empresarial</p> <p>Documento Maestro del Modelo de Seguridad y Privacidad de la Información</p> <p>Guía para la administración del riesgo y el diseño de controles en entidades públicas del Departamento Administrativo Función Pública</p> <p>Resolución 2140 de 2017 del Ministerio de Ambiente y Desarrollo Sostenible</p> <p>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</p> <p>Decreto 1499 de 2017 "Por medio del cual se modifica el Decreto 1083 de 2015, Decreto Único Reglamentario del Sector Función Pública, en lo relacionado con el Sistema de Gestión establecido en el artículo 133 de la Ley 1753 de 2015"</p> <p>Resolución 2140 de 2017 "Por la cual adopta el Modelo Integrado de Planeación y Gestión y se crean algunas instancias administrativas al interior del Ministerio de Ambiente y Desarrollo Sostenible y del Fondo Nacional Ambiental, y se dictan otras disposiciones"</p>

5. PROCEDIMIENTO

5. GESTIONAR LA ARQUITECTURA DE SEGURIDAD DE LA INFORMACIÓN



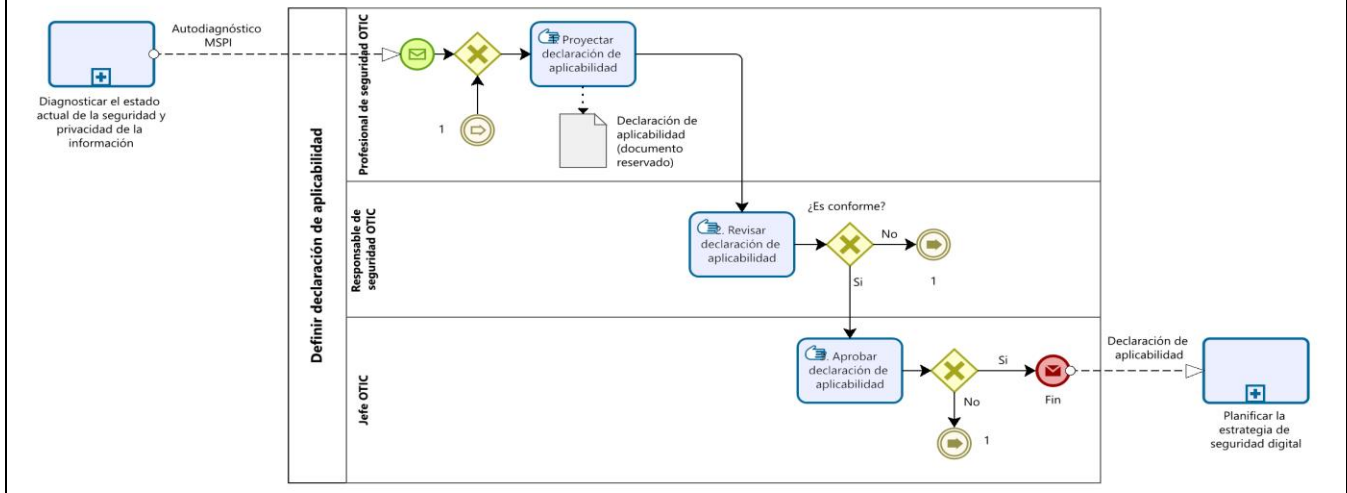
5.1.1. DIAGNOSTICAR EL ESTADO ACTUAL DE LA SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN



5.1.2. 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	El Profesional de Seguridad debe 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		Autodiagnóstico MSPi (Documento reservado)
2	Revisar el autodiagnóstico del MSPi	V	El Jefe OTIC debe revisar el instrumento del autodiagnóstico del MSPi Es conforme? Si, Continuar con la actividad 3. No, Continuar con la actividad 1.	Jefe OTIC		Autodiagnóstico MSPi - Revisado
3	Presentar ante el Comité de Gestión y Desempeño	H	El Profesional de Seguridad debe presentar el documento de Autodiagnóstico MSPi ante el Comité Institucional de Gestión y Desempeño.	Profesional de Seguridad		Autodiagnóstico MSPi presentado ante el Comité de Gestión y Desempeño
4	Aprobar Autodiagnóstico del MSPi	V	El Comité de Gestión y Desempeño debe revisar y aprobar el documento autodiagnóstico MSPi. ¿Es conforme? Si, Fin de la etapa. No, Continuar con la actividad 1.	Comité de Gestión y Desempeño	X	F-E-SIG-25 Acta de reunión - Autodiagnóstico MSPi - Aprobado

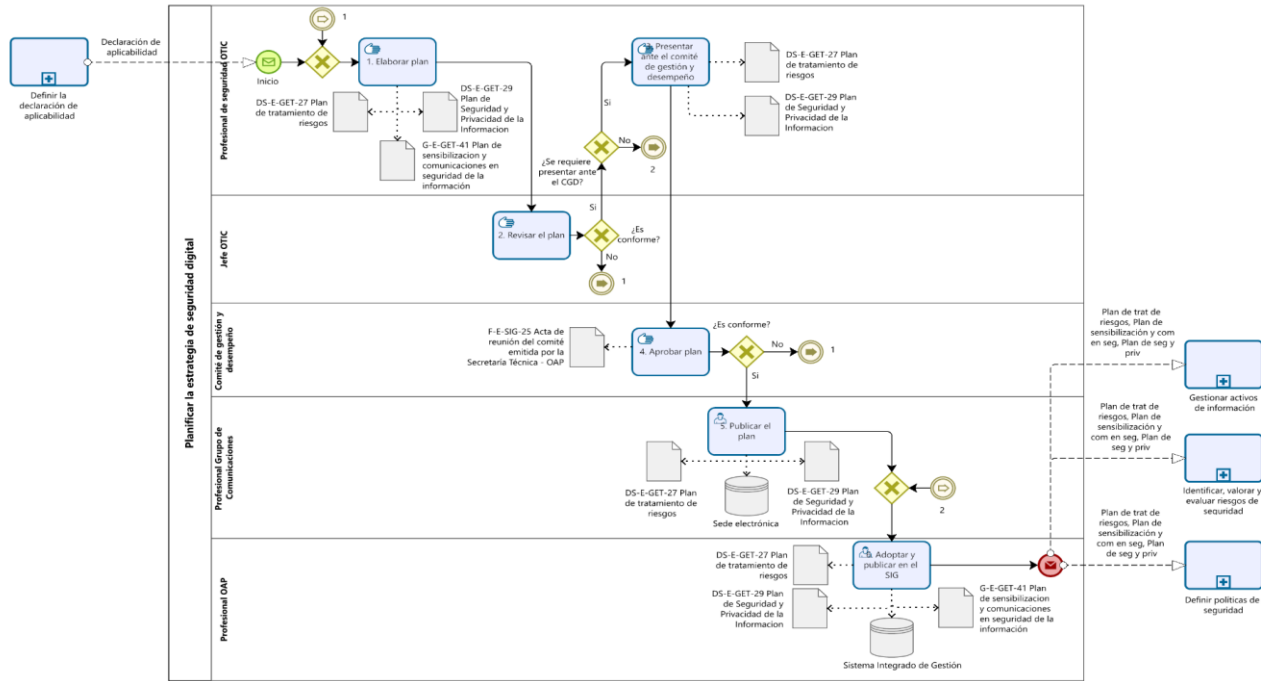
5.2.1. DEFINIR DECLARACIÓN DE APLICABILIDAD



5.2.2. DEFINIR DECLARACIÓN DE APLICABILIDAD

N.º	ACTIVIDAD	CICLO PHVA	DESCRIPCIÓN	RESPONSABLE	PC	REGISTRO
1	Proyectar declaración de aplicabilidad	H	El Profesional de Seguridad OTIC debe proyectar la declaración de aplicabilidad con las justificaciones de la aplicación de los controles, así como la justificación de las exclusiones.	Profesional de Seguridad OTIC		Declaración de aplicabilidad (documento reservado)
2	Revisar declaración de aplicabilidad	V	El Responsable de Seguridad OTIC debe revisar el documento de Declaración de Aplicabilidad de acuerdo con los controles identificados. ¿Es conforme? Si, Continuar con la actividad 3. No, Continuar con la actividad 1.	Responsable de Seguridad OTIC		Declaración de aplicabilidad (documento reservado) - Revisado
3	Aprobar declaración de aplicabilidad	A	El Jefe OTIC debe aprobar la Declaración de aplicabilidad. ¿Es conforme? Si, Fin de la etapa. No, Continuar con la actividad 1.	Jefe OTIC	X	Declaración de aplicabilidad (documento reservado) Aprobado

5.3.1. PLANIFICAR LA ESTRATEGIA DE SEGURIDAD DIGITAL

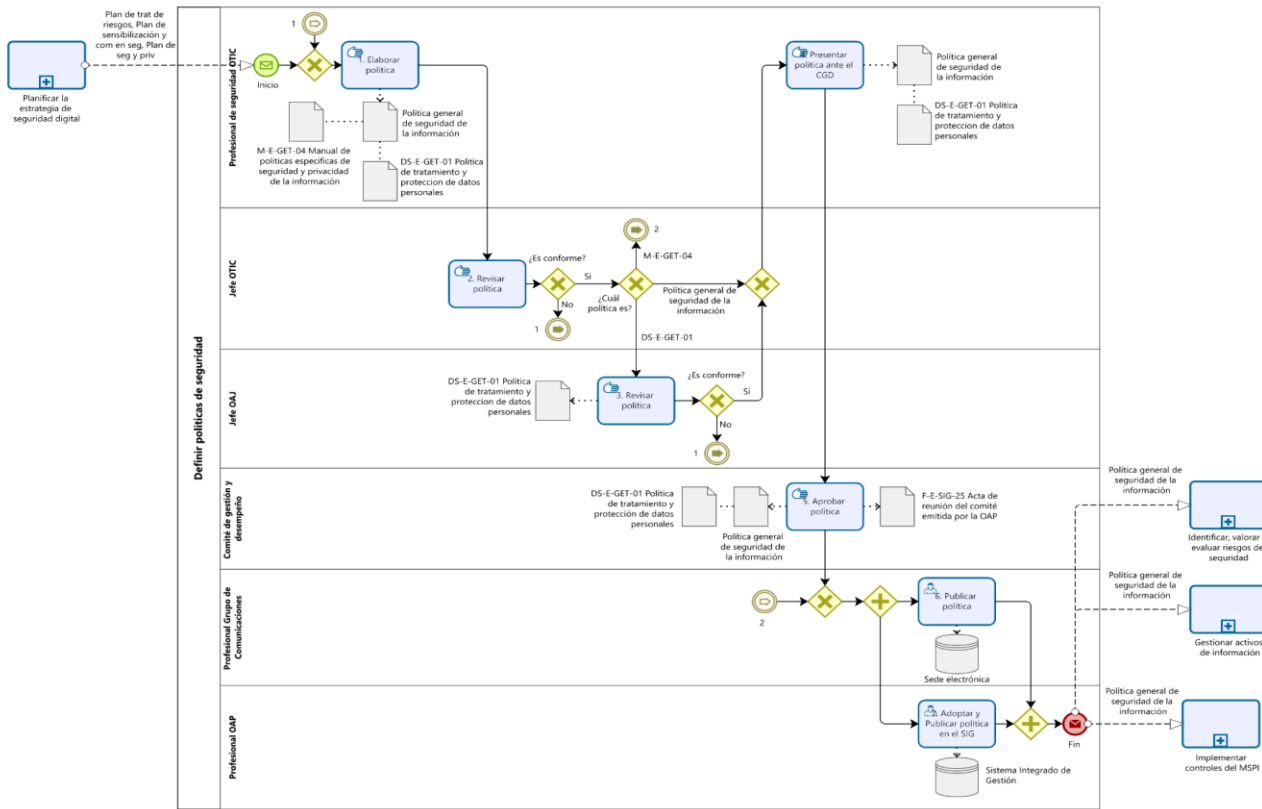


5.3.2. ACTIVIDADES PLANIFICAR LA ESTRATEGIA DE SEGURIDAD DIGITAL

N.º	ACTIVIDAD	CICLO PHVA	DESCRIPCIÓN	RESPONSABLE	PC	REGISTRO
1	Elaborar plan	H	El Profesional de Seguridad OTIC debe elaborar el Plan de Tratamiento de Riesgos, el 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		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)
2	Revisar el plan	V	El Jefe de la Oficina de Tecnologías de la Información y la Comunicación (OTIC) debe revisar el plan (Plan de Tratamiento de Riesgos, el Plan de Sensibilización y Comunicaciones en Seguridad de la Información) y dar su Vo. Bo. de conformidad. ¿Es conforme? Si, Continuar con siguiente pregunta No, Continuar con la actividad 1 ¿Se requiere presentar ante el Comité de Gestión y Desempeño - CGD? Si, Continuar con actividad 3. No, Continuar con actividad 6. Nota: Los planes que requieren ser presentados ante el CGD son DS-E-GET-27 Plan de tratamiento de Riesgos y DS-E-GET-29 Plan de Seguridad y Privacidad de la Información	Jefe OTIC	X	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 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 Plan de Tratamiento de Riesgos y el Plan de Seguridad y Privacidad de la Información los cuáles se someterán a aprobación.	Profesional de Seguridad OTIC		DS-E-GET-27 Plan de tratamiento de Riesgos, DS-E-GET-29 Plan de Seguridad y Privacidad de la Información - Presentado(s)
4	Aprobar plan	V	El Comité de Gestión y Desempeño debe revisar y aprobar los planes (Plan de Tratamiento de Riesgos y el Plan de Seguridad y Privacidad de la Información). ¿Es conforme? No, Continuar con la actividad 1. Si, Continuar con actividad 5.	Comité de Gestión y Desempeño	X	F-E-SIG-25 Acta de reunión del comité emitida por la Secretaría Técnica - Oficina Asesora de Planeación

5	Publicar el plan	A	El Profesional del Grupo de Comunicaciones debe publicar el plan (Plan de Tratamiento de Riesgos y el Plan de Seguridad y Privacidad de la Información) en sede electrónica.	Profesional Grupo de Comunicaciones	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	Profesional de la Oficina Asesora Planeación debe publicar los planes en el Sistema Integrado de Gestión Fin de la etapa.	Profesional Oficina Asesora Planeación OAP	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 - Publicado(s) en el Sistema Integrado de Gestión

5.4.1. DEFINIR POLÍTICAS DE SEGURIDAD

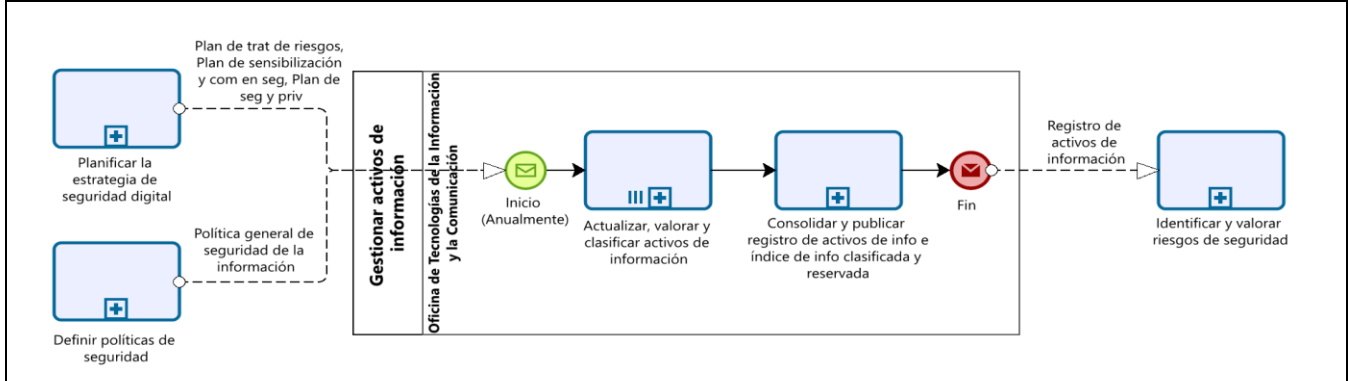


5.4.2. DEFINIR POLÍTICAS DE SEGURIDAD

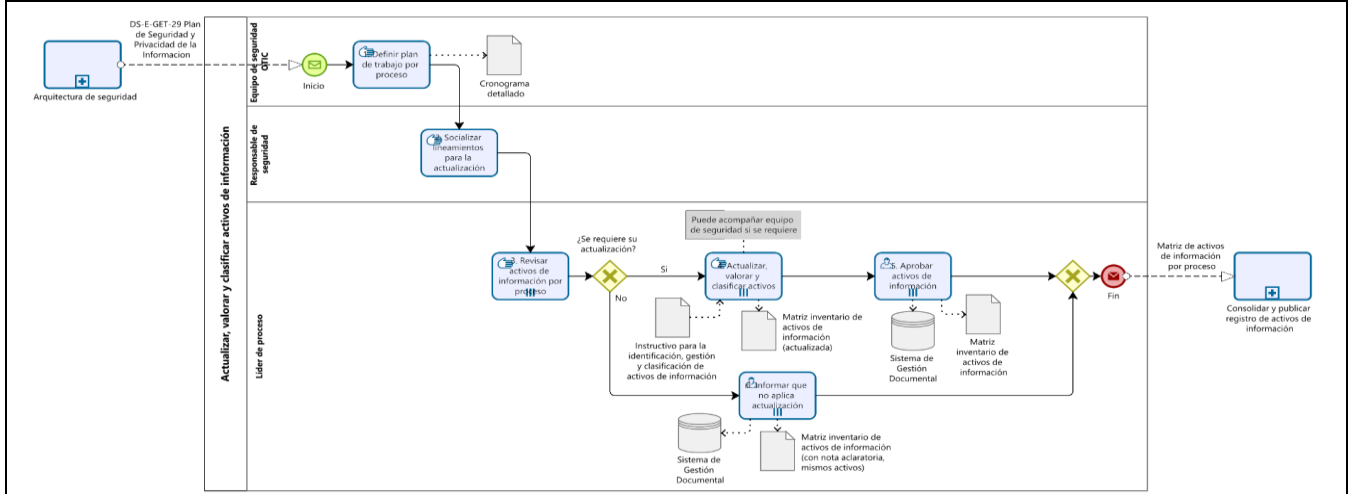
N.º	ACTIVIDAD	CICLO PHVA	DESCRIPCIÓN	RESPONSABLE	PC	REGISTRO
1	Elaborar política	H	El Profesional de Seguridad debe elaborar o actualizar la política (Política general de seguridad de la información, DS-E-GET-01 Política de tratamiento y protección de datos personales y/o M-E-GET-04 Manual de políticas 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		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 - Elaborada
2	Revisar política	V	El Jefe de la Oficina de Tecnologías de la Información y la Comunicación (OTIC) debe revisar la Política ¿Es conforme? No, Continuar con la actividad 1. Si, ¿Cuál política es? DS-E-GET-01, Continuar con actividad 3. Política general de seguridad de la información, Continuar con actividad 4. M-E-GET-04, Continuar con actividad 6 y 7 de manera paralela.	Jefe OTIC	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 - Revisada

3	Revisar política	V	El Jefe de la Oficina Asesora Jurídica debe revisar de manera integral la DS-E-GET-01 Política de tratamiento y protección de datos personales ¿Es conforme? No, Continuar con actividad 1 Si, Continuar con actividad 4.	Jefe Oficina Asesora Jurídica	DS-E-GET-01 Política de tratamiento y protección de datos personales - Revisada	
4	Presentar política ante Comité de Gestión y Desempeño	H	Profesional de Seguridad deberá 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 de Gestión y Desempeño para su aprobación.	Profesional de Seguridad	Política general de seguridad de la información y/o DS-E-GET-01 Política de Tratamiento y Protección de Datos Personales - Revisada en CGD	
5	Aprobar política	V	El Comité de Gestión y Desempeño debe 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	F-SIG-25 Acta de reunión del comité emitida por la Secretaría Técnica - Oficina Asesora de Planeación
6	Publicar política	A	El Profesional del Grupo de Comunicaciones debe publicar la política aprobada en la sede electrónica. Fin de la etapa.	Profesional Grupo de Comunicaciones		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 - Publicada en sede electrónica
7	Adoptar y Publicar política en el SIG	A	El Profesional de la Oficina Asesora de Planeación - OAP debe publicar la política aprobada en el Sistema Integrado de Gestión Fin de la etapa.	Profesional Oficina Asesora de Planeación - OAP		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 - Publicada en el Sistema Integrado de Gestión

5.5.1. GESTIONAR ACTIVOS DE INFORMACIÓN



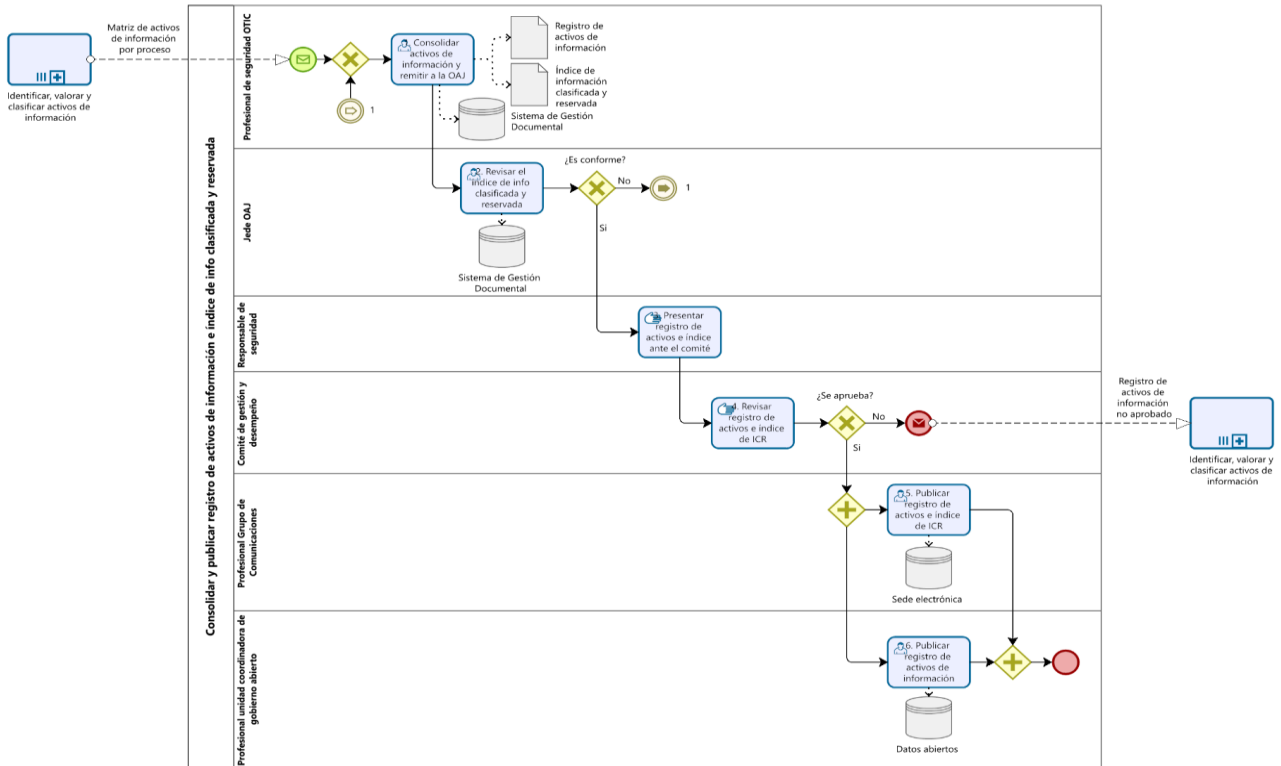
5.5.1.1 ACTUALIZAR, VALORAR Y CLASIFICAR ACTIVOS DE INFORMACIÓN



MINISTERIO DE AMBIENTE Y DESARROLLO SOSTENIBLE	GESTIONAR LA ARQUITECTURA DE SEGURIDAD DE LA INFORMACIÓN	SOMOSIG Sistema Integrado de Gestión
	Proceso: Gestión Estratégica de Tecnologías de la Información	
Versión: 1	Vigencia: 19/10/2023	Código: P-E-GET-15

5.5.1.2 ACTUALIZAR, VALORAR Y CLASIFICAR ACTIVOS DE INFORMACIÓN						
N.º.	ACTIVIDAD	CICLO PHVA	DESCRIPCIÓN	RESPONSABLE	PC	REGISTRO
1	Definir plan de trabajo por proceso	P	El Equipo de Seguridad de la OTIC 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	Cronograma de trabajo
2	Socializar lineamientos para la actualización	H	El Responsable de Seguridad debe socializar los lineamientos para la actualización de los activos de información a los líderes de proceso y/o sus delegados.	Responsable de Seguridad	X	F-E-SIG-05 Listado de asistencia o grabación o listado de asistencia Teams o correo electrónico o pieza comunicativa.
3	Revisar activos de información por proceso	H	El Líder de proceso y/o su delegado, debe 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-I-E-GET-02 Metodología para la identificación, gestión y clasificación de activos de información ¿Se requiere su actualización? Si, Continuar con actividad 4 No, Continuar con actividad 6.	Líder de Proceso		F-E-GET-18 Matriz inventario de activos de información Ministerio de Ambiente y Desarrollo Sostenible – AMBIENTE
4	Actualizar, valorar y clasificar activos	V	El Líder de proceso y/o su delegado, debe actualizar, valorar y clasificar los activos de información que lo requieran conforme al I-E-GET-02 Metodología para la identificación, gestión y clasificación de activos de información.	Líder de Proceso		F-E-GET-18 Matriz inventario de activos de información Ministerio de Ambiente y Desarrollo Sostenible – AMBIENTE
5	Aprobar activos de información	H	El Líder de Proceso debe 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.	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 actualizada - Radicados en el sistema de gestión documental.
6	Informar que no aplica actualización por el Sistema de Gestión Documental	H	El Líder de proceso debe 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.	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 CONSOLIDAR Y PUBLICAR REGISTRO DE ACTIVOS DE INFORMACIÓN E ÍNDICE DE INFORMACIÓN CLASIFICADA Y RESERVADA

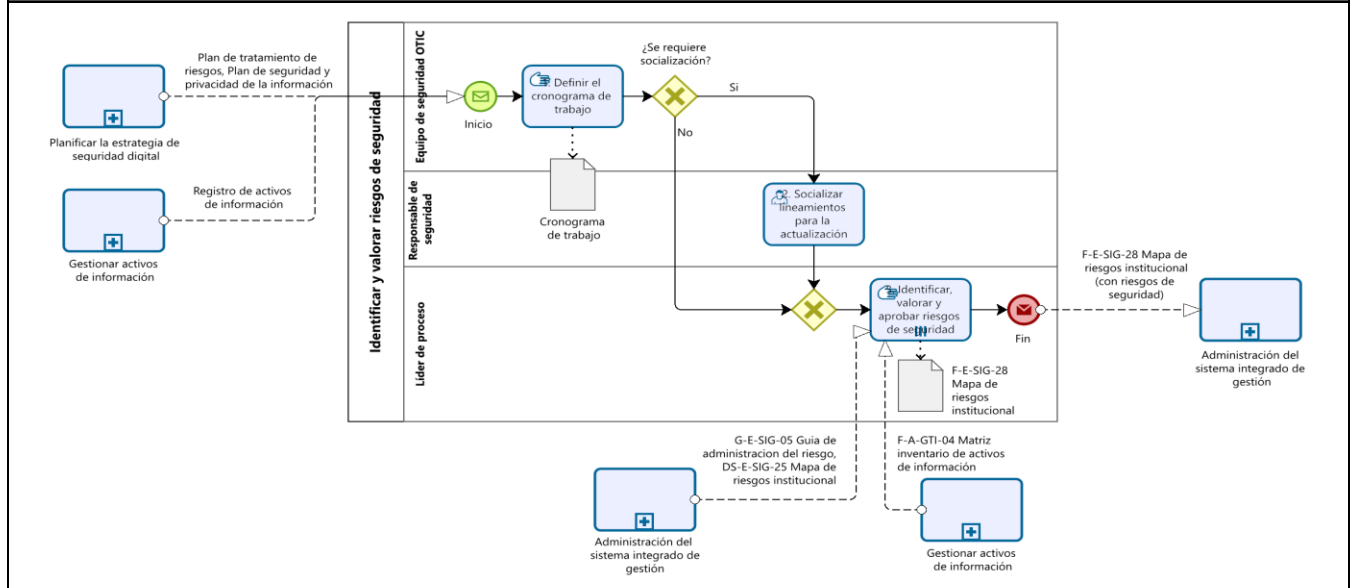


5.5.2.2 CONSOLIDAR Y PUBLICAR REGISTRO DE ACTIVOS DE INFORMACIÓN E ÍNDICE DE INFORMACIÓN CLASIFICADA Y RESERVADA

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 Matriz Inventario de Activos de Información 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 el Información Clasificada y Reservada para revisión por parte de la Oficina Asesora Jurídica.	Profesional de Seguridad OTIC		Registro de Activos de Información Índice de Información Clasificada y Reservada radicado en sistema de gestión documental
2	Revisar el índice de información clasificada y reservada	V	El Jefe de la Oficina Asesora Jurídica debe 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. No, Continuar con actividad 1.	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 Comité Institucional de Gestión y Desempeño	H	El Responsable de Seguridad debe 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.	Responsable de Seguridad		Presentación de consolidado de datos del Registro de Activos de Información e Índice de Información Clasificada y Reservada
4	Revisar y aprobar el registro de activos e Índice de Información clasificada y reservada	V	El Comité de Gestión y Desempeño debe revisar y aprobar el Índice de Información Clasificada y Reservada y el Registro de Activos de Información. ¿Se aprueba? No, Continuar con la actividad 1 del subproceso Identificar, valorar y clasificar activos de información. Si, Continuar con la actividad 5 y 6 de manera paralela.	Comité de Gestión y Desempeño		F-E-SIG-25 Acta de reunión del comité emitida por la Secretaría Técnica - Oficina Asesora de Planeación Acto administrativo que de aprobación a los activos de información

5	Publicar registro de activos e Índice de Información Clasificada y Reservada	A	El Responsable de seguridad de la entidad debe 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. El Profesional del Grupo de Comunicaciones debe publicar los documentos mencionados en la sede electrónica del Ministerio. Nota: El Grupo de comunicaciones publica los documentos consolidados en el mismo formato enviado por el Responsable de seguridad.	Profesional Grupo de Comunicaciones	X	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

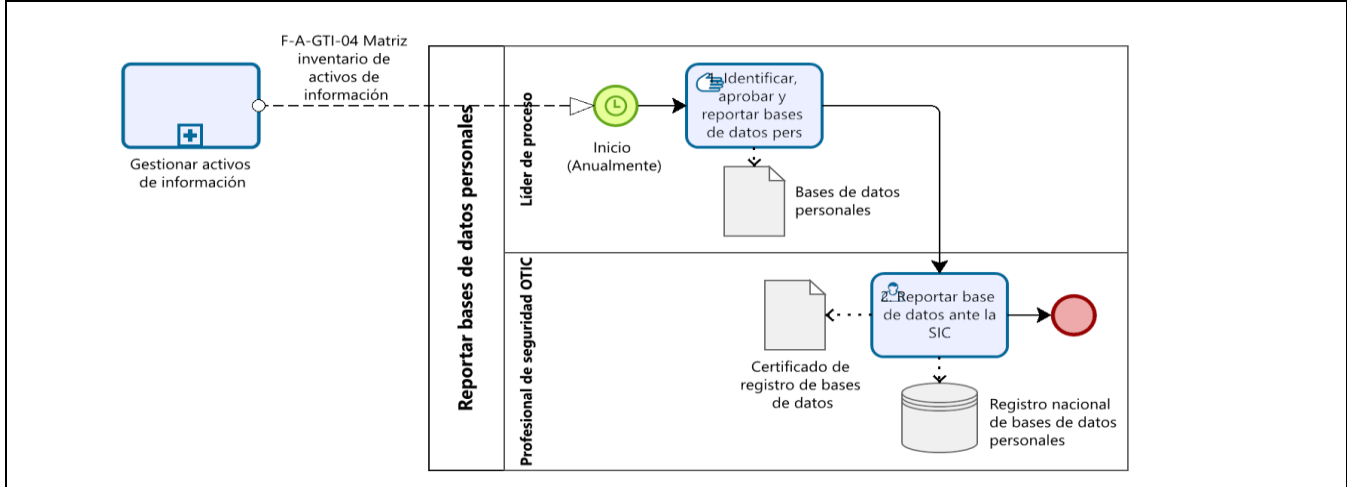
5.6.1. IDENTIFICAR Y VALORAR RIESGOS DE SEGURIDAD



5.6.2. IDENTIFICAR Y VALORAR RIESGOS DE SEGURIDAD

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

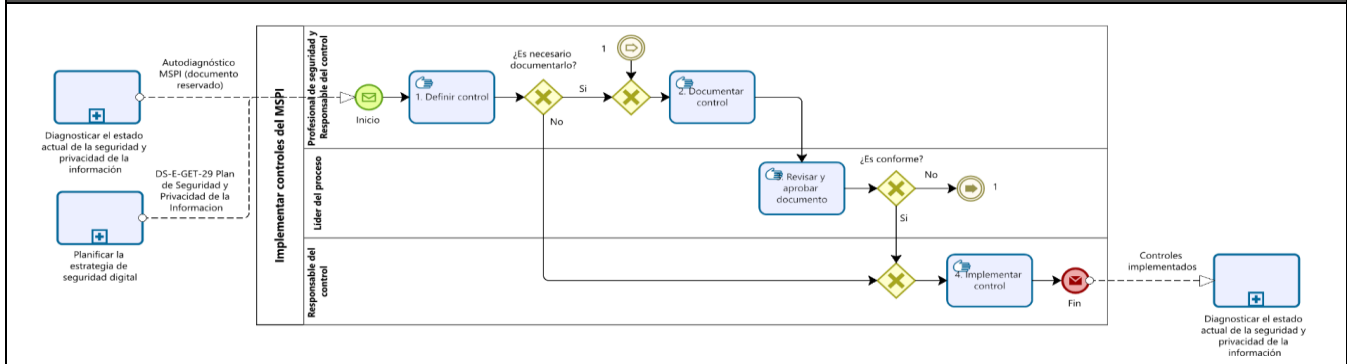
5.7.1. REPORTAR BASES DE DATOS PERSONALES



5.7.2. REPORTAR BASES DE DATOS PERSONALES


N.º	ACTIVIDAD	CICLO PHVA	DESCRIPCIÓN	RESPONSABLE	PC	REGISTRO
1	Identificar, aprobar y reportar bases de datos personales	H	El Líder de proceso y/o su delegado, debe identificar en la Matriz inventario de activos de información las bases de datos personales reportadas y consignar la información en el formato de Reporte de bases de datos personales. Esta actividad debe realizarse anualmente.	Lider de Proceso		F-E-GET-10 Reporte de bases de datos personales
2	Reportar Base de Datos en la SIC	A	Profesional de Seguridad debe reportar la base de datos en el Registro nacional de bases de datos personales en la SIC. SIC emite un Certificado como constancia del reporte las bases de datos. Fin del Subproceso.	Profesional de Seguridad OTIC	X	Certificado de registro de bases de datos

5.8.1 IMPLEMENTAR CONTROLES DEL MSPI



5.8.2 IMPLEMENTAR CONTROLES DEL MSPI

N.º	ACTIVIDAD	CICLO PHVA	DESCRIPCIÓN	RESPONSABLE	PC	REGISTRO
1	Definir control	P	El Profesional de Seguridad y el Responsable del Control deben definir el mecanismo y el delegado para implementar controles del MSPI. ¿Es necesario documentarlo? Si, Continuar con la actividad 2. No, Continuar con la actividad 4.	Profesional de Seguridad Responsable del Control		Control definido
2	Documentar control	H	El Profesional de Seguridad y el Responsable del Control deben documentar los controles del MSPI.	Profesional de Seguridad Responsable del Control		Control documentado
3	Revisar y aprobar documento	V	El Líder de Proceso debe revisar y aprobar el documento con los controles del MSPI. ¿Es conforme? Si, Continuar con la actividad 4. No, Continuar con la actividad 2.	Lider de Proceso	X	Control revisado
4	Implementar control	A	El Responsable debe implementar el control de acuerdo con lo definido en el documento MSPI.	Responsable del Control	X	Control implementado

MINISTERIO DE AMBIENTE Y DESARROLLO SOSTENIBLE	GESTIONAR LA ARQUITECTURA DE SEGURIDAD DE LA INFORMACIÓN	 Sistema Integrado de Gestión
	Proceso: Gestión Estratégica de Tecnologías de la Información	
Versión: 1	Vigencia: 19/10/2023	Código: P-E-GET-15

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.