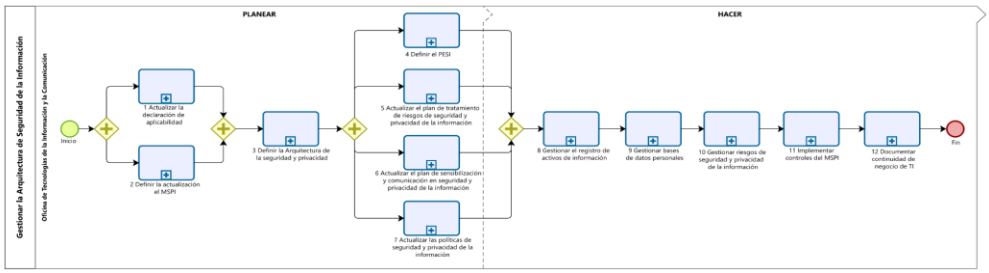
MINISTERIO DE AMBIENTE Y DESARROLLO SOSTENIBLE	**GESTIONAR LA ARQUITECTURA DE SEGURIDAD DE LA INFORMACIÓN** **Proceso:** Gestión Estratégica de Tecnologías de la Información	SOMOS IG Sistema Integrado de Gestión
Versión: 3	**Vigencia:** 29/12/2025	**Código:** P-E-GET-15

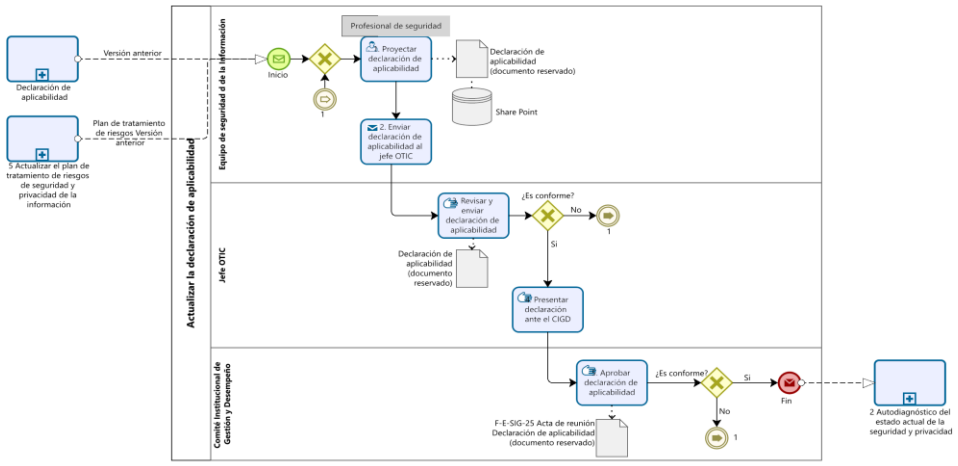
1. OBJETIVO(S)	Documentar y gestionar el Modelo de Seguridad y Privacidad de la Información, el Sistema de Gestión de Seguridad de la Información, la Arquitectura de seguridad del Marco de Referencia de Arquitectura Empresarial y demás lineamientos en términos de seguridad de la Información que deba cumplir el Ministerio de Ambiente y Desarrollo Sostenible.
2. ALCANCE	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 DE LA INFORMACIÓN** El Comité Institucional de Gestión y Desempeño asegurará la implementación, seguimiento y mejora continua de las políticas de gestión y de las directrices en materia de seguridad digital y seguridad de la información, impartidas por la Presidencia de la República y el Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC), de conformidad con lo establecido en la Resolución 2140 de 2017 y demás normas que la modifiquen o sustituyan. **PROTECCIÓN DE ACTIVOS DE INFORMACIÓN** La entidad, sus colaboradores y terceros se comprometen a proteger adecuadamente los activos de información, en especial aquellos clasificados como confidenciales, con el fin de preservar los principios de confidencialidad, integridad y disponibilidad. Para tal efecto, se adoptan y aplican los lineamientos definidos en la Metodología para la identificación, gestión y clasificación de activos de información, mediante la cual se establecen mecanismos de protección acordes con la clasificación de la información: Información Pública, Información Pública Clasificada e Información Pública Reservada. • El Grupo de Gestión Documental acompañará el levantamiento, validación y consolidación de los activos de información cuando los líderes de proceso o los profesionales de seguridad de la OTIC lo consideren necesario, de acuerdo con las funciones establecidas en la I-E-GET-02 Metodología para la identificación, gestión y clasificación de activos de información. •El Índice de Información Clasificada y Reservada será revisado y aprobado por la Oficina Jurídica. **REPORTE Y GESTIÓN DE BASES DE DATOS PERSONALES** Los líderes de proceso, jefes de oficina y coordinadores de grupo son responsables de identificar, actualizar, reportar y, cuando aplique, solicitar la eliminación de las bases de datos personales que se encuentren bajo su administración y que ya no sean necesarias para el cumplimiento de las funciones misionales o administrativas. Esta actividad deberá realizarse anualmente, y la OTIC será la encargada de centralizar, cargar y registrar la información correspondiente en la Plataforma de la Superintendencia de Industria y Comercio (SIC), dentro de los plazos establecidos para esta obligación legal. **DECLARACIÓN DE APLICABILIDAD (SOA)** La entidad deberá elaborar, mantener actualizada y documentada la Declaración de Aplicabilidad (Statement of Applicability – SOA), instrumento mediante el cual se determinan los controles de seguridad implementados, parcialmente implementados o no implementados, así como su respectiva justificación. La SOA deberá ser revisada, aceptada y aprobada por la jefatura de la OTIC, y constituirá un insumo clave para la gestión de riesgos y la mejora continua del Sistema de Seguridad de la Información. **GESTIÓN DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN** El Ministerio deberá implementar la gestión de riesgos de seguridad y privacidad de la información conforme a los lineamientos establecidos en la Guía para la administración del riesgo de la Oficina Asesora de Planeación en su versión vigente, así como en el Anexo Técnico del Modelo Nacional de Riesgos en las Entidades Públicas, incluyendo sus actualizaciones periódicas. Se deberá asegurar la identificación, análisis, evaluación y tratamiento de los riesgos que puedan generar pérdida de confidencialidad, integridad, disponibilidad y privacidad de la información, y que afecten la continuidad de las operaciones institucionales. Para ello, se deberá formular y mantener actualizado el plan de tratamiento de riesgos, con responsables, plazos y controles definidos. **ACUERDO DE NIVEL DE SERVICIO PARA PUBLICACIÓN DE INFORMACIÓN** El Acuerdo de Nivel de Servicio (ANS) del Grupo de Comunicaciones para la publicación de documentos en la sede electrónica de la entidad será de tres (3) días hábiles, contados a partir de la recepción completa y validada de la solicitud correspondiente.
4. NORMAS Y DOCUMENTOS DE REFERENCIA	•ISO/IEC 27001/2022: Sistema de Gestión de Seguridad de la Información – Requisitos. • ISO/IEC 27002/2022: Seguridad de la información, ciberseguridad y protección de la privacidad – Controles de seguridad de la información. Norma que define un conjunto de controles y buenas prácticas actualizadas para la gestión de la seguridad de la información. • CONPES 3854 de 2016: Política Nacional de Seguridad Digital, que establece los lineamientos para la gestión de riesgos digitales, el fortalecimiento de capacidades y la protección de los activos digitales del Estado. • Marco de Referencia de Arquitectura Empresarial – MRAE: Documento Maestro del Marco de Referencia de Arquitectura Empresarial del Estado colombiano, que orienta la alineación de los procesos, la información, los sistemas y la tecnología con la estrategia institucional. • Modelo de Seguridad y Privacidad de la Información (MSPI): Documento Maestro del Modelo definido por el MinTIC, en su versión vigente, que establece los lineamientos, dominios y controles para la gestión de la seguridad y privacidad de la información en las entidades públicas. • Guía para la administración del riesgo y el diseño de controles en entidades públicas: Emitida por el Departamento Administrativo de la Función Pública (DAFP), en su versión vigente, que define los lineamientos metodológicos para la identificación, análisis, evaluación y tratamiento de los riesgos institucionales, incluidos los riesgos de seguridad de la información. • 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. • Decreto 612 de 2018: Por el cual se fijan directrices para la integración de los planes institucionales y estratégicos al Plan de Acción de las entidades del Estado, incorporando la gestión de la seguridad digital y de la información dentro de la planeación institucional. • Decreto 1008 de 2018: Por el cual se establece la Política de Gobierno Digital, que integra la seguridad digital como un habilitador transversal para la transformación digital del Estado. • Ley 1581 de 2012: Y sus decretos reglamentarios Régimen general de protección de datos personales, aplicable al tratamiento de la información personal administrada por las entidades públicas. •Ley 1712 de 2014: Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional, que define las categorías de información pública, clasificada y reservada. • Resolución 500 de 2021: Es una norma emitida por el Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC) que establece los lineamientos y estándares para la estrategia de seguridad digital, e instituye el Modelo de Seguridad y Privacidad de la Información (MSPI) como habilitador de la Política de Gobierno Digital. • Resolución 02277 de 2025: actualiza el MSPI adoptando los lineamientos de la ISO/IEC 27001:2022 y ajustando disposiciones anteriores para alinearlas con mejores prácticas internacionales.

5. PROCEDIMIENTO

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



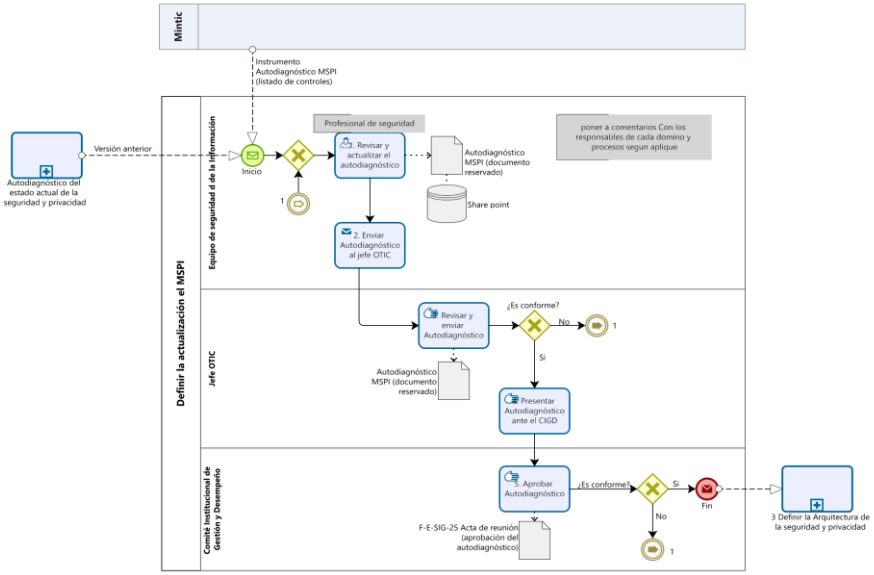
5.1.1. FLUJOGRAMA "ACTUALIZAR LA DECLARACIÓN DE APLICABILIDAD"



5.1.2. ACTIVIDADES "ACTUALIZAR LA DECLARACIÓN DE APLICABILIDAD"

N.º.	ACTIVIDAD	CICLO PHVA	DESCRIPCIÓN	RESPONSABLE	PC	REGISTRO
1	Proyectar declaración de aplicabilidad	**H**	Proyectar la Declaración de Aplicabilidad (SoA) del Sistema de Gestión de Seguridad de la Información, documentando de manera clara y trazable las justificaciones para la adopción, implementación o exclusión de los controles de seguridad de la información, de conformidad con los resultados del análisis y valoración de riesgos, el alcance definido del SGSI, así como los cambios identificados en el entorno normativo, institucional y tecnológico.	Equipo de Seguridad de la Información		Documento Declaración de aplicabilidad- **Actualizado** en el Share Point
2	Enviar declaración de aplicabilidad al jefe OTIC	**H**	El profesional de Seguridad o su delegado Remitirá, vía correo electrónico, el Documento de Declaración de Aplicabilidad (SoA) al Jefe de la OTIC para su revisión y aprobación.	Equipo de Seguridad de la Información		Correo electrónico **Enviado**
3	Revisar y enviar declaración de aplicabilidad	**V**	Revisar, validar y remitir la Declaración de Aplicabilidad (SoA) al Comité Institucional de Gestión y Desempeño. ¿Es conforme? **Si:** Continua con la actividad 4 "Presentar declaración ante el CIGD" **No:** Continua con la actividad 1 "Proyectar declaración de aplicabilidad"	Jefe OTIC	**X**	Documento Declaración de aplicabilidad - **Revisado**
4	Presentar declaración ante el CIGD	**H**	El jefe de la OTIC o su delegado Deberá presentar la Declaración de Aplicabilidad (SoA) ante el Comité Institucional de Gestión y Desempeño (CIGD).	Jefe OTIC		N/A
5	Aprobar declaración de aplicabilidad	**A**	Aprobar la Declaración de Aplicabilidad (SoA) por parte del Comité Institucional de Gestión y Desempeño (CIGD) ¿Es conforme? **Si:** Fin de la Etapa **No:** Continua con la actividad 1 "Proyectar declaración de aplicabilidad" **Fin de la Etapa**	Comité Institucional de Gestión y Desempeño (CIGD)		Documento **F-E-SIG-25** – Acta de reunión del Comité Institucional de Gestión y Desempeño, con la **Aprobación** de la Declaración de Aplicabilidad (SoA)

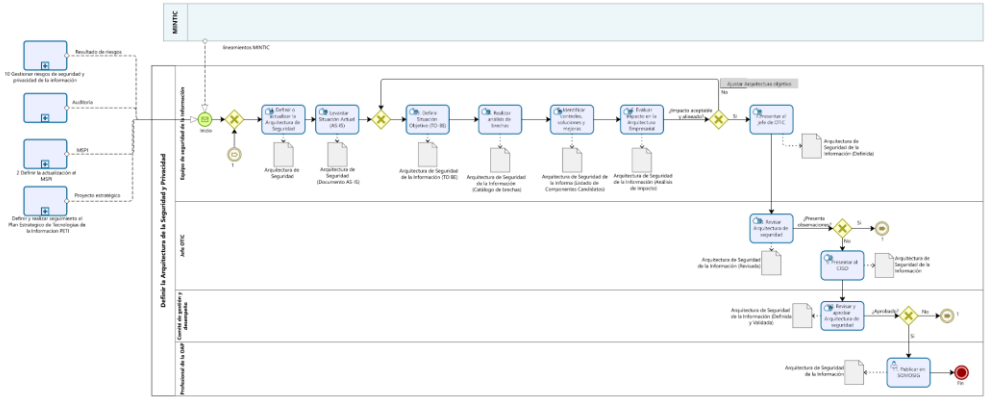
5.2.1. FLUJOGRAMA "DEFINIR LA ACTUALIZACIÓN EL MSPI"



5.2.2. ACTIVIDADES "DEFINIR LA ACTUALIZACIÓN EL MSPI"

N.º.	ACTIVIDAD	CICLO PHVA	DESCRIPCIÓN	RESPONSABLE	PC	REGISTRO
1	Revisar y actualizar el autodiagnóstico	**H**	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).	Equipo de Seguridad de la Información		Documento Autodiagnóstico MSPI **Diligenciado** - Share Point
2	Enviar autodiagnóstico al Jefe OTIC	**H**	El profesional de Seguridad o su delegado Remitirá, vía correo electrónico, el Documento Autodiagnóstico MSPI al Jefe de la OTIC para su revisión y aprobación.	Equipo de Seguridad de la Información		Correo electrónico Enviado
3	Revisar y enviar autodiagnóstico	**V**	Revisar el instrumento de autodiagnóstico del Modelo de Seguridad y Privacidad de la Información (MSPI) y remitir al Comité Institucional de Gestión y Desempeño (CIGD). ¿Es conforme? **Si:** Continuar con la actividad 4 "Presentar autodiagnóstico ante el Comité Institucional de Gestión y Desempeño" **No:** Continuar con la actividad 1 "Revisar y actualizar el autodiagnóstico"	Jefe OTIC	**X**	Documento Autodiagnóstico MSPI - **Revisado**
4	Presentar autodiagnóstico ante el CIGD	**H**	El jefe de la OTIC o su delegado Deberá presentar Autodiagnóstico MSPI ante el Comité Institucional de Gestión y Desempeño (CIGD).	Jefe OTIC		N/A
5	Aprobar autodiagnóstico	**A**	Revisar y aprobar el documento autodiagnóstico MSPI. ¿Es conforme? **Si:** Fin de la etapa **No:** Continuar con la actividad 1 "Revisar y actualizar el autodiagnóstico". **Nota:** Esta acción se realiza cuantas veces sea necesario hasta lograr la aprobación. **Fin de la etapa.**	Comité Institucional de Gestión y Desempeño (CIGD)		Documento **F-E-SIG-25** – Acta de reunión del Comité Institucional de Gestión y Desempeño, con la **Aprobación** del autodiagnóstico MSPI

5.3.1. FLUJOGRAMA "DEFINIR LA ARQUITECTURA DE LA SEGURIDAD Y PRIVACIDAD "

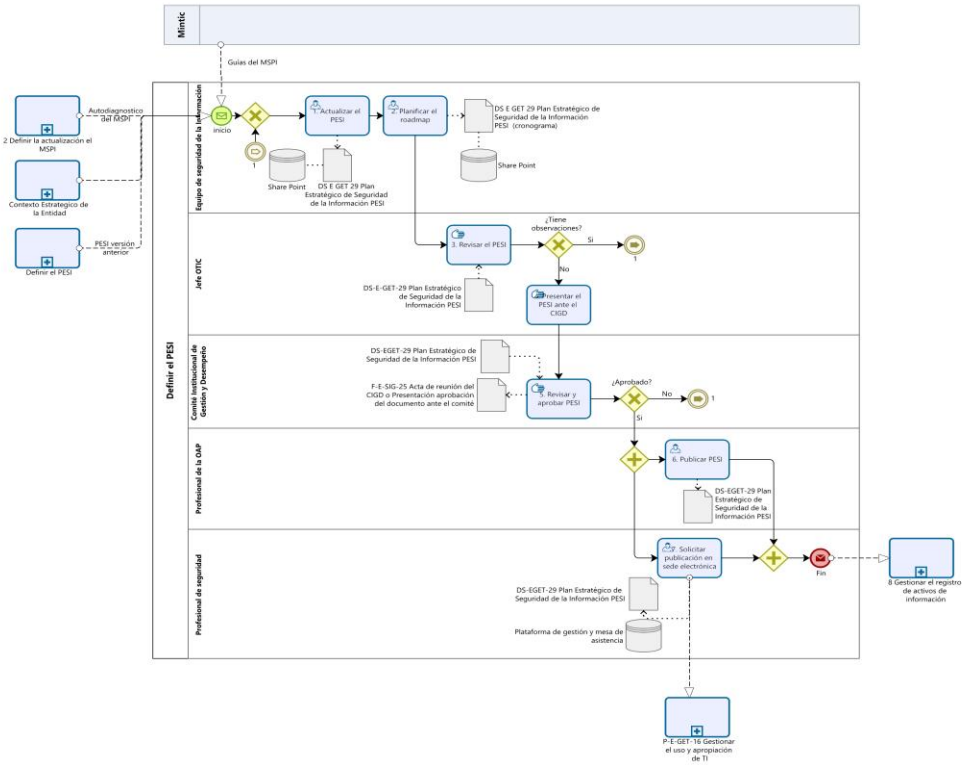


5.3.2. ACTIVIDADES "DEFINIR LA ARQUITECTURA DE LA SEGURIDAD Y PRIVACIDAD "

N.º.	ACTIVIDAD	CICLO PHVA	DESCRIPCIÓN	RESPONSABLE	PC	REGISTRO
1	Definir o actualizar la Arquitectura de Seguridad	**H**	Consultar el repositorio de arquitectura empresarial para identificar y reutilizar modelos, lineamientos, aplicables a la Arquitectura de Seguridad de la Información. Definir o actualizar la Arquitectura de Seguridad de la Información, garantizando la coherencia entre controles de seguridad, activos de información, servicios tecnológicos y riesgos, conforme a los lineamientos institucionales y normativos vigentes.	Equipo de Seguridad de la Información		Arquitectura de Seguridad - **Definida**
2	Levantar Situación Actual (AS-IS)	**H**	Documentar la Arquitectura de Seguridad de la Información en su estado actual, definiendo las vistas conceptual, lógica y física, mediante la identificación del contexto regulatorio, los activos de información, los servicios y componentes de seguridad, los riesgos a alto nivel y las tecnologías de seguridad implementadas.	Equipo de Seguridad de la Información		Catalogo de activos de información Catalogo de política de seguridad Catalogo de regulación Matriz de riesgos Componentes de seguridad Servicios de seguridad Diagrama de zonas de seguridad y comunicaciones Catalogo tecnologías de seguridad
3	Definir Situación Objetivo (TO-BE)	**H**	Definir la Arquitectura de Seguridad de la Información en su estado futuro, alineada con las preocupaciones institucionales, mediante la identificación de los atributos institucionales que actúan como motivadores de seguridad, el desarrollo de las vistas de arquitectura para la situación objetivo y la definición de los servicios y componentes de seguridad requeridos para su implementación. Incluye las tareas: •Definir arquitectura contextual •Definir arquitectura conceptual •Definir arquitectura lógica •Definir arquitectura física •Definir arquitectura de componentes •Definir arquitectura operacional	Equipo de Seguridad de la Información		Vista de la capa empresarial. Comprender los requisitos institucionales (RI) de las partes interesad Vista de capa de arquitectura. Diseño conceptual para cumplir con BR y estrategia de diseño. Vista de capa de diseño. Entrega de “servicios” e “información” para cumplir con el concepto. Vista de capa de construcción. Entrega de elementos tangibles para apoyar los servicios lógicos. Vista de comerciante. Hardware, herramientas y estándares para entregar el diseño físico vista Administrador de servicios. Cómo gestionamos la arquitectura.
4	Realizar análisis de brechas	**H**	Comparar la situación actual con la situación objetivo para determinar las capacidades faltantes y proponer componentes candidatos.	Equipo de Seguridad de la Información		Arquitectura de Seguridad - (Catálogo de Brechas)
5	Identificar controles, soluciones y mejoras	**H**	•Identificar controles, soluciones y mejoras. •Asociar a brechas.	Equipo de Seguridad de la Información		Arquitectura de Seguridad con listado de Componentes Candidatos
6	Evaluar impacto en la Arquitectura Empresarial	**V**	Evaluar el impacto derivado de la implementación de controles, soluciones y mejoras de seguridad de la información. ¿Impacto aceptable y alineado? **Si:** Continua con la actividad 7 "Presentar al jefe de OTIC" **No:** Continua con la actividad 3 "Definir Situación Objetivo (TO-BE)"	Equipo de Seguridad de la Información	**X**	Análisis de impacto de la Arquitectura de Seguridad documentado
7	Presentar al jefe de OTIC	**H**	Presentación de la Arquitectura de Seguridad al Jefe de la OTIC	Equipo de Seguridad de la Información		N/A

8	Revisar Arquitectura de seguridad	**V**	Arquitectura de Seguridad de la Información revisada ¿Presenta observaciones? **Si:** Continua con la actividad 1 " Definir o actualizar la Arquitectura de Seguridad" **No:** Continua con la actividad 9 "Presentar al CIGD"	Jefe OTIC		Arquitectura de Seguridad definida y documentada
9	Presentar al CIGD	**H**	Arquitectura de Seguridad de la Información presentada al Comité Institucional de Gestión y Desempeño	Jefe OTIC		N/A
10	Revisar y aprobar Arquitectura de seguridad	**A**	Realizar una Revisión Formal con los Interesados para asegurar la comprensión de la situación objetivo y las decisiones tomadas. ¿Aprobado? **Si:** Continua con la actividad 1 " Definir o actualizar la Arquitectura de Seguridad" **No:** Continua con la actividad 11 "Publicar en SOMOSIG"	Comité Institucional de Gestión y Desempeño		Documento **F-E-SIG-25** – Acta de reunión del Comité Institucional de Gestión y Desempeño, con la Arquitectura de Seguridad **Definida y Validada**
11	Publicar en SOMOSIG	**H**	Publicar la Arquitectura de Seguridad de la Información aprobada en la plataforma SOMOSIG, asegurando su correcta versionamiento, disponibilidad y acceso	Profesional de la OAP		Documento Arquitectura de Seguridad - Actualizado en SOMOSIG

5.4.1. FLUJOGRAMA "DEFINIR EL PESI "

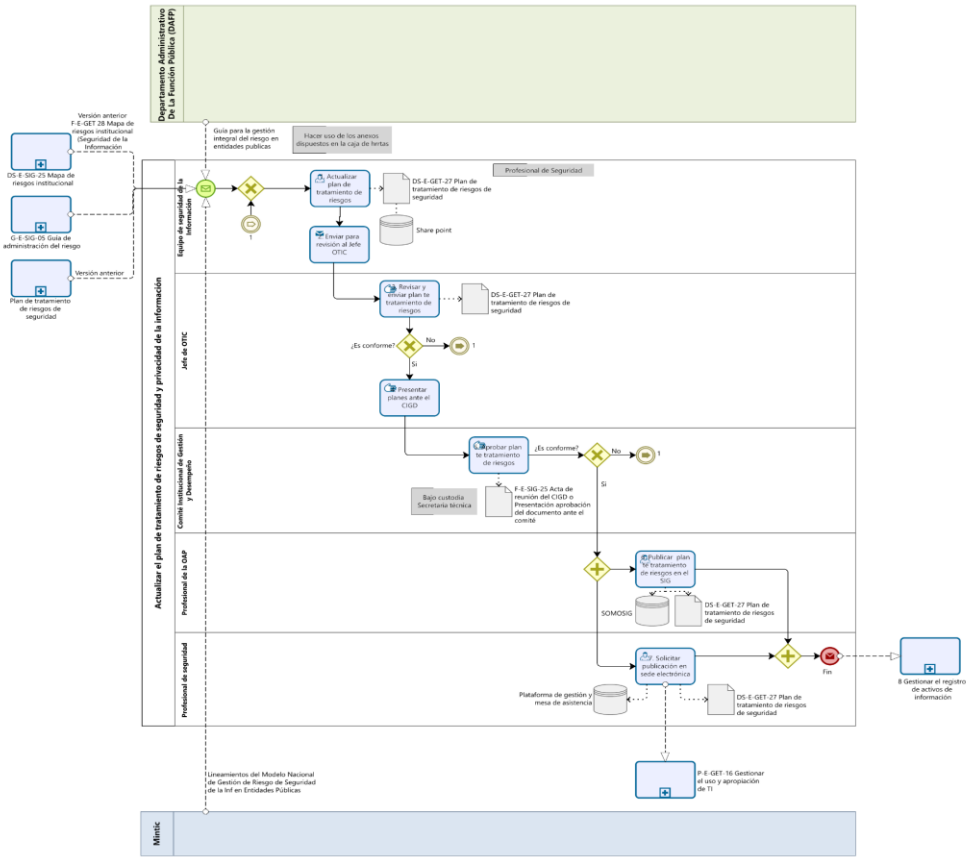


5.4.2. ACTIVIDADES "DEFINIR EL PESI "

N.º.	ACTIVIDAD	CICLO PHVA	DESCRIPCIÓN	RESPONSABLE	PC	REGISTRO
1	Actualizar el PESI	**H**	Actualizar el Plan Estratégico de Sistemas de Información (PESI) conforme al contexto institucional, el marco estratégico y normativo vigente, los resultados de los análisis institucionales y la evolución del entorno tecnológico	Equipo de Seguridad de la Información		Documento **DS-E-GET-29** Plan Estratégico de Seguridad de la Información PESI (borrador) **Actualizad**o en Share Point
2	Planificar el roadmap	**H**	Planificar el roadmap, indicando iniciativas, responsables, hitos y cronograma.	Equipo de Seguridad de la Información		Documento **DS-E-GET-29** Plan Estratégico de Seguridad de la Información PESI (cronograma) **Definido** en Share Point
3	Revisar el PESI	**V**	Revisar el PESI y su roadmap con el fin de verificar su alineación estratégica. ¿Tiene observaciones? **Si:** Continua con la actividad 1 "Actualizar el PESI" **No:** Continua con la actividad 4 "Presentar el PESI ante el CIGD"	Jefe OTIC	**X**	Documento **DS-E-GET-29** Plan Estratégico de Seguridad de la Información PESI - **Revisado**

4	Presentar el PESI ante el CIGD	**H**	El jefe de la OTIC o su delegado Deberá presentar **DS-E-GET-29** Plan Estratégico de Seguridad de la Información PESI ante el Comité Institucional de Gestión y Desempeño (CIGD).	Jefe OTIC		N/A
5	Revisar y aprobar PESI	**A**	Revisar y aprobar el documento **DS-E-GET-29** Plan Estratégico de Seguridad de la Información PESI ¿Aprobado? **Si:** Continua con las actividades 6 y 7 paralelamente "Publicar PESI" y "Solicitar publicación en sede electrónica" **No:** Continuar con la actividad 1 "Actualizar el PESI".	Comité Institucional de Gestión y Desempeño (CIGD)		Documento **F-E-SIG-25** – Acta de reunión del Comité Institucional de Gestión y Desempeño, con la **Aprobación** del **DS-E-GET-29** Plan Estratégico de Seguridad de la Información PESI
6	Publicar PESI	**H**	Actualizar documento **DS-E-GET-29** Plan Estratégico de Seguridad de la Información PESI - Aprobado en el aplicativo Sistema Integrado - SOMISIG	Profesional de la OAP	**X**	Documento **DS-E-GET-29** Plan Estratégico de Seguridad de la Información PESI - **Actualizado** en SOMOSIG
7	Solicitar publicación en sede electrónica	**H**	Solicitar al Profesional de Uso y Apropiación - OTIC la publicación del documento **DS-E-GET-29** Plan Estratégico de Seguridad de la Información PESI - aprobado en la sede electrónica de la Entidad, conforme a los lineamientos del procedimiento **P-E-GET-16** Gestionar el uso y apropiación de TI. **Fin de la etapa**.	Profesional de Seguridad	**X**	Caso - **Solicitado** en la Plataforma de gestión y mesa de asistencia

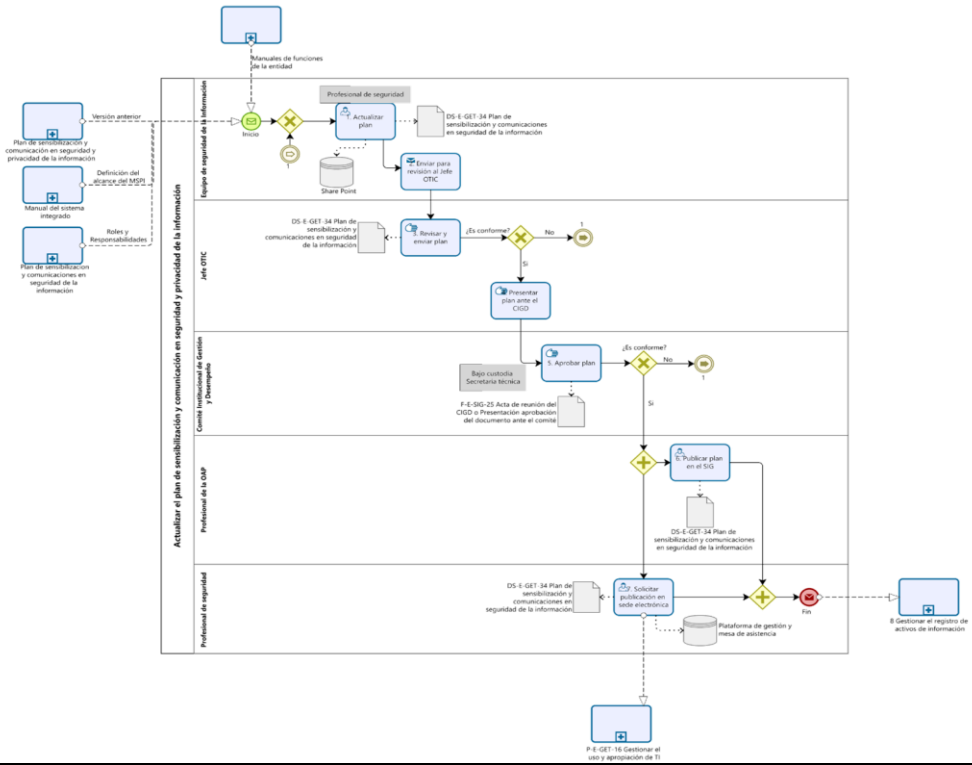
5.5.1. FLUJOGRAMA "ACTUALIZAR EL PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN"



5.5.2. ACTIVIDADES "ACTUALIZAR EL PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN"

N.º.	ACTIVIDAD	CICLO PHVA	DESCRIPCIÓN	RESPONSABLE	PC	REGISTRO
1	Actualizar plan de tratamiento de riesgos	**H**	Actualizar el **DS-E-GET-27** Plan de tratamiento de riesgos de seguridad , con base en los resultados de la identificación, análisis y valoración de riesgos, de conformidad con la Guía para la Gestión Integral del Riesgo en Entidades Públicas, haciendo uso de los anexos y formatos dispuestos en la Caja de Herramientas institucional, y definiendo las opciones de tratamiento, los controles aplicables, los responsables y los plazos de implementación.	Equipo de Seguridad de la Información		**DS-E-GET-27** Plan de tratamiento de riesgos de seguridad **Actualizado** - Share Point
2	Enviar para revisión al Jefe OTIC	**H**	El profesional de Seguridad o su delegado Remitirá, vía correo electrónico, el Documento **DS-E-GET-27** Plan de tratamiento de riesgos de seguridad al Jefe de la OTIC para su revisión y aprobación.	Equipo de Seguridad de la Información		Correo electrónico Enviado
3	Revisar y enviar plan de tratamiento de riesgos	**V**	Revisar el **DS-E-GET-27** Plan de tratamiento de riesgos de seguridad y remitirlo al Comité Institucional de Gestión y Desempeño ¿Es conforme? **Si:** Continua con la actividad 4 "Presentar planes ante el CIGD" **No:** Continua con la actividad 1 "Actualizar plan de tratamiento de riesgos"	Jefe de OTIC	**X**	**DS-E-GET-27** Plan de tratamiento de riesgos de seguridad - **Revisado**
4	Presentar planes ante el CIGD	**H**	El Jefe de la OTIC o su delegado deberá presentar ante el Comité Institucional de Gestión y Desempeño (CIGD) el **DS-E-GET-27** Plan de Tratamiento de Riesgos de Seguridad de la Información, para su conocimiento, análisis y toma de decisiones	Jefe de OTIC		N/A
5	Aprobar plan de tratamiento de riesgos	**A**	Aprobar el **DS-E-GET-27** Plan de tratamiento de riesgos de seguridad en el marco del Comité Institucional de Gestión y Desempeño (CIGD). ¿Es conforme? **Si:** Continua paralelamente con las actividades 6 "Publicar plan te tratamiento de riesgos en el SIG" y 7 "Solicitar publicación en sede electrónica" **No:** Continua con la actividad 1 "Actualizar plan de tratamiento de riesgos"	Comité Institucional de Gestión y Desempeño		Documento **F-E-SIG-25** – Acta de reunión del Comité Institucional de Gestión y Desempeño, con la **Aprobación** del **DS-E-GET-27** Plan de tratamiento de riesgos de seguridad
6	Publicar plan de tratamiento de riesgos en el SIG	**H**	Publicar el Documento **DS-E-GET-27** Plan de tratamiento de riesgos de seguridad aprobado en el Sistema Integrado de Gestión, garantizando el control de versión.	Profesional de la OAP	**X**	Documento **DS-E-GET-27** Plan de tratamiento de riesgos de seguridad - aprobado - **Publicado** en SOMOSIG
7	Solicitar publicación en sede electrónica	**H**	Solicitar a través de GEMA la publicación del documento **DS-E-GET-27** Plan de tratamiento de riesgos de seguridad aprobado en la sede electrónica de la Entidad. conforme a los lineamientos del procedimiento P-E-GET-16 Gestionar el uso y apropiación de TI **Fin de la etapa**	Profesional de seguridad	**X**	Caso - **Solicitado** en la Plataforma de gestión y mesa de asistencia

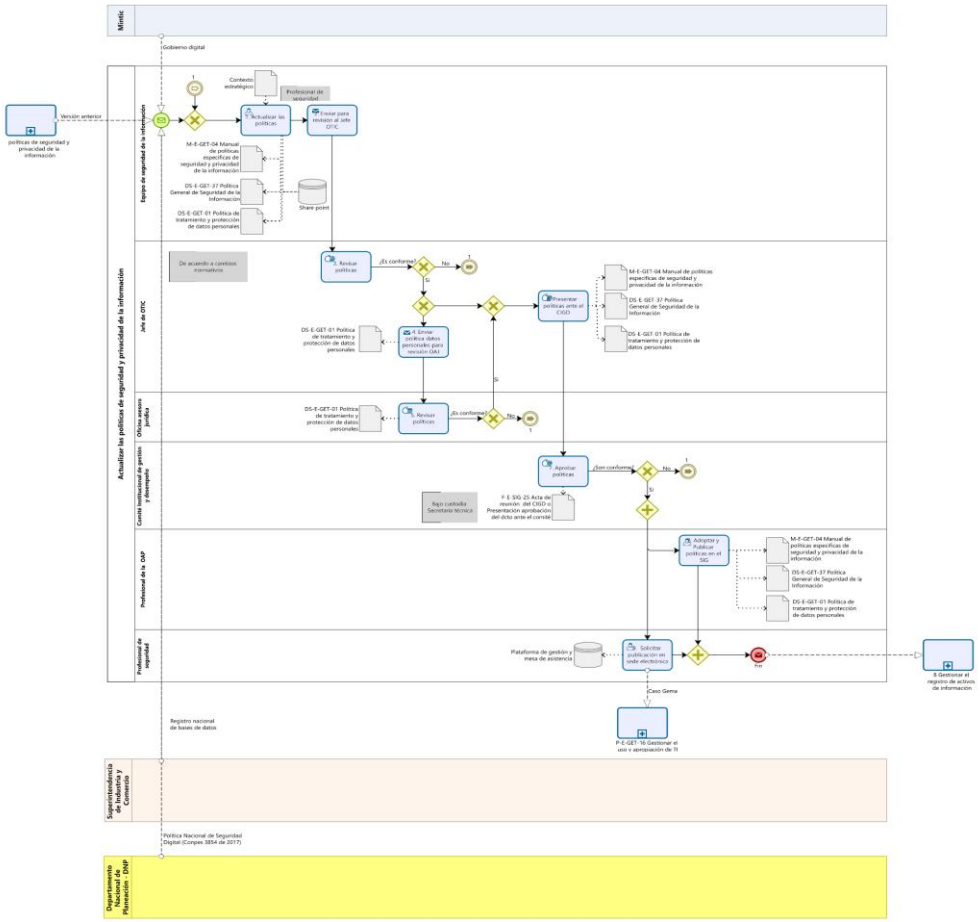
5.6.1. FLUJOGRAMA "ACTUALIZAR EL PLAN DE SENSIBILIZACIÓN Y COMUNICACIÓN EN SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN"



5.6.2. ACTIVIDADES "ACTUALIZAR EL PLAN DE SENSIBILIZACIÓN Y COMUNICACIÓN EN SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN"

N.º.	ACTIVIDAD	CICLO PHVA	DESCRIPCIÓN	RESPONSABLE	PC	REGISTRO
1	Actualizar plan	**H**	Actualizar el **DS-E-GET-34** – Plan de Sensibilización y Comunicaciones en Seguridad de la Información.	Equipo de Seguridad de la Información		Documento **DS-E-GET-34** – Plan de Sensibilización y Comunicaciones en Seguridad de la Información **Actualizado** en Share Point
2	Enviar para revisión al Jefe OTIC	**H**	El profesional de seguridad o su delegado debe remitir vía correo electrónico el **DS-E-GET-34** – Plan de Sensibilización y Comunicaciones en Seguridad de la Información al Jefe de la OTIC, para su revisión y aprobación del cronograma y de los contenidos de sensibilización propuestos.	Equipo de Seguridad de la Información		Correo electrónico Enviado
3	Revisar y enviar plan	**V**	Revisar el **DS-E-GET-34** – Plan de Sensibilización y Comunicaciones en Seguridad de la Información y enviar al Comité Institucional de Gestión y Desempeño	Jefe OTIC	**X**	Documento **DS-E-GET-34 –** Plan de Sensibilización y Comunicaciones en Seguridad de la Información - **Revisado**
4	Presentar plan ante el CIGD	**H**	El jefe de la OTIC o su delegado debe Presentar el **DS-E-GET-34 –** Plan de Sensibilización y Comunicaciones en Seguridad de la Información ante el Comité Institucional de Gestión y Desempeño (CIGD), para su aprobación.	Jefe OTIC		N/A
5	Aprobar plan	**A**	Aprobar el **DS-E-GET-34 –** Plan de Sensibilización y Comunicaciones en Seguridad de la Información en el marco del Comité Institucional de Gestión y Desempeño (CIGD). ¿Es conforme? **Si:** Continua paralelamente con las actividades 6 y 7 "Publicar plan te tratamiento de riesgos en el SIG" y "Solicitar publicación en sede electrónica" **No:** Continua con la actividad 1 "Actualizar plan de tratamiento de riesgos"	Comité Institucional de Gestión y Desempeño		Documento **F-E-SIG-25** – Acta de reunión del Comité Institucional de Gestión y Desempeño, con la **Aprobación** del **DS-E-GET-34 –** Plan de Sensibilización y Comunicaciones en Seguridad de la Información
6	Publicar plan en el SIG	**H**	Publicar el Documento **DS-E-GET-34 –** Plan de Sensibilización y Comunicaciones en Seguridad de la Información aprobado en el Sistema Integrado de Gestión, garantizando el control de versión.	Profesional de la OAP	**X**	Documento **DS-E-GET-34 –** Plan de Sensibilización y Comunicaciones en Seguridad de la Información - aprobado - **Publicado** en SOMOSIG
7	Solicitar publicación en sede electrónica	**H**	Solicitar a través de GEMA la publicación del documento **DS-E-GET-34 –** Plan de Sensibilización y Comunicaciones en Seguridad de la Información aprobado en la sede electrónica de la Entidad. conforme a los lineamientos del procedimiento **P-E-GET-16** Gestionar el uso y apropiación de TI **Fin de la etapa**	Profesional de Seguridad	**X**	Caso - **Solicitado** en la Plataforma de gestión y mesa de asistencia

5.7.1. FLUJOGRAMA "ACTUALIZAR LAS POLÍTICAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN"

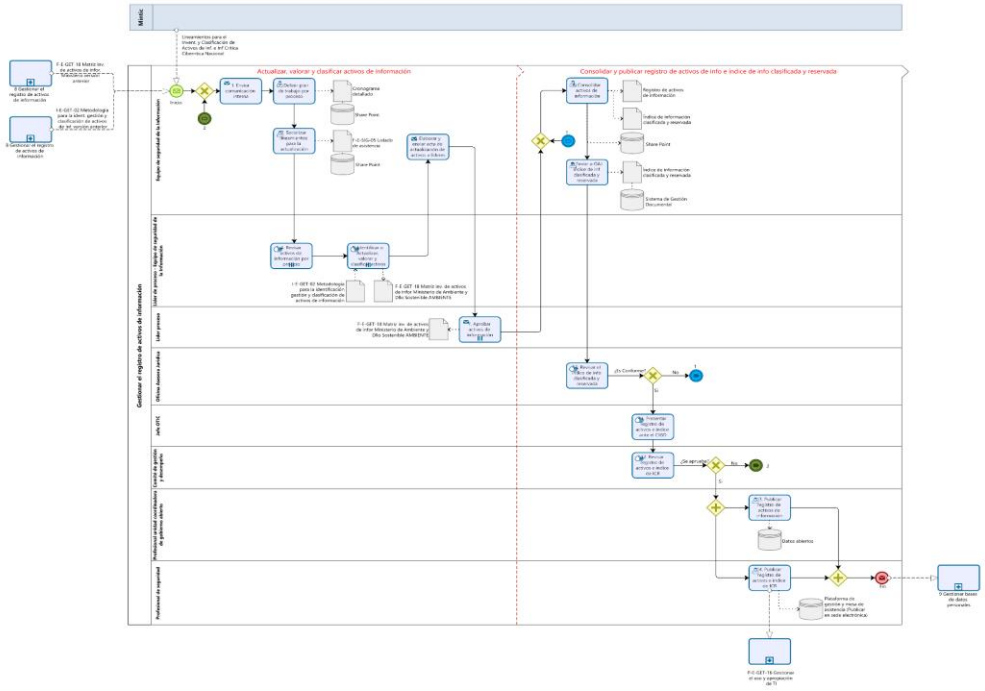


5.7.2. ACTIVIDADES "ACTUALIZAR LAS POLÍTICAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN"

N.º.	ACTIVIDAD	CICLO PHVA	DESCRIPCIÓN	RESPONSABLE	PC	REGISTRO
1	Actualizar las políticas	**H**	Realizar la revisión y actualización integral de las políticas institucionales de seguridad de la información, teniendo en cuenta: Cambios normativos vigentes (MSPI, Gobierno Digital, Ley 1581 de 2012, decretos y lineamientos MinTIC). Resultados del análisis de riesgos y del autodiagnóstico del MSPI. Observaciones de auditorías internas o externas. Cambios en el contexto organizacional, tecnológico o de procesos.	Equipo de Seguridad de la Información		Documentos (**M-E-GET-04** Manual de políticas especificas de seguridad y privacidad de la información, **DS-E-GET-37** Política General de Seguridad de la Información y **DS-E-GET-01** Política de tratamiento y protección de datos personales) **Actualizadas** - Share Point
2	Enviar para revisión al Jefe OTIC	**H**	Una vez actualizadas las políticas, El Profesional de Seguridad o su delegado debe remitirlas por correo electrónico al Jefe de la OTIC, para su revisión técnica	Equipo de Seguridad de la Información		Correo electrónico
3	Revisar políticas	**V**	Revisar cada una de las políticas de seguridad y privacidad de la información, con el fin de verificar su vigencia, coherencia normativa. ¿Es conforme? **Si:** Continua con la actividad 4 "Enviar política datos personales para revisión OAJ" y 6 "Presentar políticas ante el CIGD" **No:** Continua con la actividad 1 "Actualizar las políticas"	Jefe de OTIC	**X**	Documentos (**M-E-GET-04** Manual de políticas especificas de seguridad y privacidad de la información, **DS-E-GET-37** Política General de Seguridad de la Información y **DS-E-GET-01** Política de tratamiento y protección de datos personales) - **Revisadas**

4	Enviar política datos personales para revisión OAJ	**H**	**DS-E-GET-01** Política de Tratamiento y Protección de Datos Personales se remite a la Oficina Asesora Jurídica (OAJ) para su revisión legal.	Jefe de OTIC		**F-E-SIG-23** Memorando Interno a través de ARCA
5	Revisar políticas	**V**	Revisar **DS-E-GET-01** Política de Tratamiento y Protección de Datos Personales y enviar a la OTIC con su Vo. Bo. ¿Es conforme? **Si:** Continua con la actividad 6 "Presentar políticas ante el CIGD" **No:** Continua con la actividad 1 "Actualizar las políticas"	Oficina Asesora Jurídica	**X**	Documento **DS-E-GET-01** Política de tratamiento y protección de datos personales - Revisada
6	Presentar políticas ante el CIGD	**H**	Las políticas ajustadas y validadas técnica y jurídicamente son presentadas ante el Comité Institucional de Gestión y Desempeño (CIGD) para La adopción formal como políticas institucionales	Jefe de OTIC		N/A
7	Aprobar políticas	**A**	Formalizar la aprobación de las políticas por parte del Comité Institucional de Gestión y Desempeño, registrando la decisión y sus condiciones en el acta de la sesión	Comité Institucional de Gestión y Desempeño		Documento **F-E-SIG-25** – Acta de reunión del Comité Institucional de Gestión y Desempeño, con la **Aprobación** de las políticas (**M-E-GET-04** Manual de políticas especificas de seguridad y privacidad de la información, **DS-E-GET-37** Política General de Seguridad de la Información y **DS-E-GET-01** Política de tratamiento y protección de datos personales)
8	Adoptar y publicar políticas en el SIG	**H**	Publicar políticas (**M-E-GET-04** Manual de políticas especificas de seguridad y privacidad de la información, **DS-E-GET-37** Política General de Seguridad de la Información y **DS-E-GET-01** Política de tratamiento y protección de datos personales) aprobadas en el Sistema Integrado de Gestión.	Profesional de la OAP	**X**	Políticas (**M-E-GET-04** Manual de políticas especificas de seguridad y privacidad de la información, **DS-E-GET-37** Política General de Seguridad de la Información y **DS-E-GET-01** Política de tratamiento y protección de datos personales) - **Actualizados** en SOMOSIG
9	Solicitar publicación en sede electrónica	**H**	Solicitar a través de GEMA la publicación de los documentos **(M-E-GET-04** Manual de políticas especificas de seguridad y privacidad de la información, **DS-E-GET-37** Política General de Seguridad de la Información y **DS-E-GET-01** Política de tratamiento y protección de datos personales) aprobadas en la sede electrónica de la Entidad. conforme a los lineamientos del procedimiento **P-E-GET-16** Gestionar el uso y apropiación de TI **Fin de la etapa**	Profesional de Seguridad	**X**	Caso - **Solicitado** en la Plataforma de gestión y mesa de asistencia

5.8.1. FLUJOGRAMA "GESTIONAR EL REGISTRO DE ACTIVOS DE INFORMACIÓN"

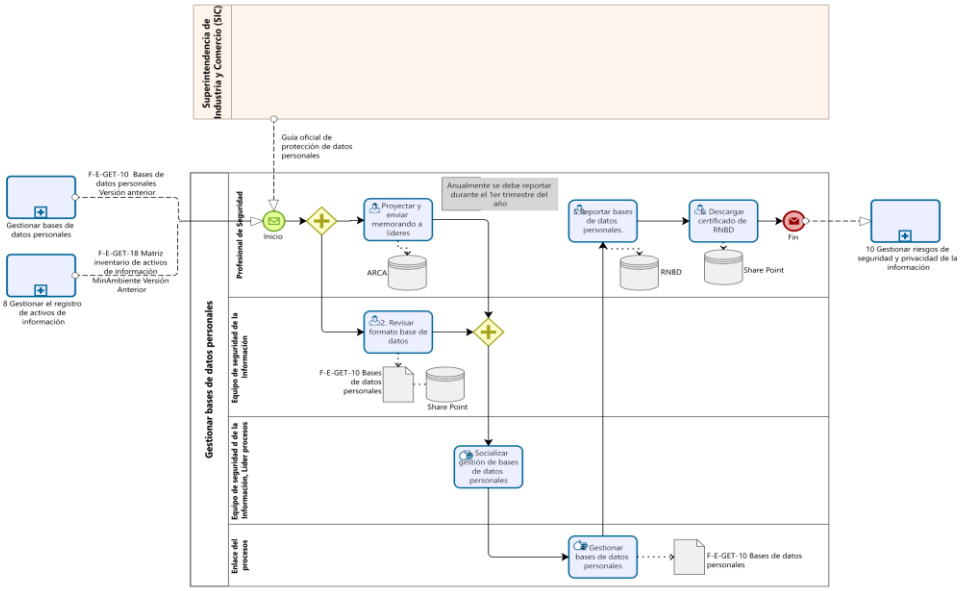


5.8.2. ACTIVIDADES "GESTIONAR EL REGISTRO DE ACTIVOS DE INFORMACIÓN"

N.º.	ACTIVIDAD	CICLO PHVA	DESCRIPCIÓN	RESPONSABLE	PC	REGISTRO
1	Enviar comunicación interna	P	Enviar comunicación interna a las dependencias para dar inicio a la fase de actualización, valoración y clasificación del inventario de activos de información e información crítica, conforme a los lineamientos de ciberseguridad nacional.	Equipo de Seguridad de la Información		Correo electrónico
2	Definir plan de trabajo por proceso	H	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 de la Información		Cronograma de trabajo
3	Socializar lineamientos para la actualización	H	Deben socializar los lineamientos para la actualización de los activos de información a los líderes de proceso y/o sus delegados.	Equipo de Seguridad de la Información		**F-E-SIG-05** Listado de asistencia o grabación o listado de asistencia Teams
4	Revisar activos de información por proceso	H	Revisar el documento Matriz inventario de activos de información Ministerio de 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.	Líder de Proceso Equipo de Seguridad de la Información		N/A
5	Identificar o Actualizar, valorar y clasificar activos	H	Actualizar, valorar y clasificar los activos de información mediante el diligenciamiento del formato **F-E-GET-18** – Matriz de Inventario de Activos de Información, con el fin de garantizar su adecuada identificación, gestión y clasificación en el Ministerio, conforme a los lineamientos definidos en el **I-E-GET-02** – Metodología para la identificación, gestión y clasificación de activos de información.	Líder de Proceso Equipo de Seguridad de la Información		Documento **F-EGET-18** Matriz inventario de activos de información Ministerio de Ambiente y Desarrollo Sostenible – AMBIENTE **Actualizado** - Share Point
6	Elaborar y enviar acta de actualización de activos a líderes	H	Elaborar y remitir, mediante acta, a los líderes de las dependencias con la actualización del inventario de activos de información, adjuntando la Matriz de Inventario diligenciada en el formato establecido	Equipo de Seguridad de la Información		Documento **F-E-SIG-25 –** Acta de reunión con la **Actualización** de la **F-EGET-18** Matriz inventario de activos de información Ministerio de Ambiente y Desarrollo Sostenible – AMBIENTE
7	Aprobar activos de información	A	Los líderes de los procesos aprueban la actualización de los activos de información mediante correo electrónico remitido por el Jefe de la Oficina, como evidencia de la validación y aprobación del inventario correspondiente. **Continua con la fase de Consolidar y publicar registro de activos de información e índice de información clasificada y reservada**	Líder de Proceso	X	Correo electrónico con la aprobación del inventario de activos de información y el documento **F-EGET-18** Matriz inventario de activos de información Ministerio de Ambiente y Desarrollo Sostenible – AMBIENTE
8	Consolidar activos de información	H	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.	Equipo de Seguridad de la Información		Registro de Activos de Información - Share Point Índice de Información Clasificada y Reservada radicado en sistema de gestión documental - Share Point
9	Enviar a OAJ índice de información clasificada y reservada	H	Remitir a través del Sistema de Gestión Documental - ARCA la Información Clasificada y Reservada para revisión por parte de la Oficina Asesora Jurídica.	Equipo de Seguridad de la Información		**F-E-SIG-23** Memorando Interno a través de ARCA
10	Revisar el índice de información clasificada y reservada	V	Revisar el índice de información clasificada y reservada y emitir su visto bueno o comentarios mediante memorando. ¿Es Conforme? **Si:** Continua con la actividad 11 "Presentar registro de activos e índice ante el CIGD" **No:** Continua con la actividad 8 "Consolidar activos de información "	Oficina Asesora Jurídica	X	**F-E-SIG-23** Memorando Interno a través de ARCA
11	Presentar registro de activos e índice ante el CIGD	H	El Jefe de OTIC o su delegado 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	Jefe OTIC		N/A

12	Revisar registro de activos e índice de ICR	**A**	Revisar, en Comité, el Registro de Activos de Información y el Índice de Información Clasificada y Reservada (ICR) ¿Se aprueba? **Si:** Continua con la actividad 13 y 14 paralelamente "Publicar registro de activos de información" y "Publicar registro de activos e índice de ICR" **No:** Continua con la actividad 1 "Enviar comunicación interna"	Comité de Gestión y Desempeño		Documento **F-E-SIG-25** – Acta de reunión del Comité Institucional de Gestión y Desempeño, con la **Aprobación** del Registro de Activos de Información e Índice de Información Clasificada y Reservada
13	Publicar registro de activos de información	**H**	Publicar Registro de Activos de Información aprobado en datos abiertos	Profesional Unidad Coordinadora de Gobierno Abierto	**X**	Documento Registro de Activos de Información - **Aprobado y Publicado** en datos abiertos
14	Publicar registro de activos e índice de ICR	**H**	Solicitar a través de GEMA el Índice de Información Clasificada y Reservada publicación de aprobadas en la sede electrónica de la Entidad. conforme a los lineamientos del procedimiento **P-E-GET-16** Gestionar el uso y apropiación de TI **Fin de la etapa**.	Profesional de Seguridad	**X**	Caso - **Solicitado** en la Plataforma de gestión y mesa de asistencia

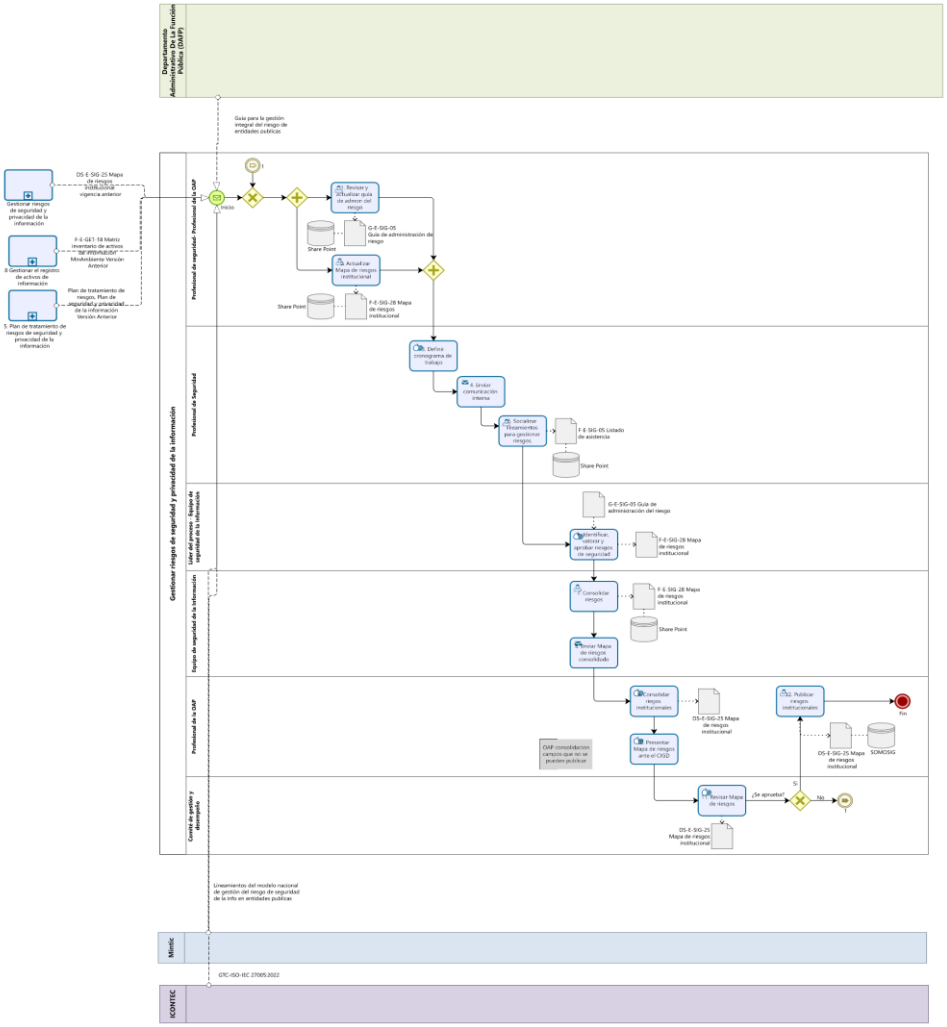
5.9.1. FLUJOGRAMA "GESTIONAR BASES DE DATOS PERSONALES"



5.9.2. ACTIVIDADES "GESTIONAR BASES DE DATOS PERSONALES"

N.º.	ACTIVIDAD	CICLO PHVA	DESCRIPCIÓN	RESPONSABLE	PC	REGISTRO
1	Proyectar y enviar memorando a líderes	**P**	Debe proyectar y remitir memorando a los líderes de las dependencias para solicitar el reporte de bases de datos personales, información que debe ser remitida durante el primer trimestre del año.	Profesional de Seguridad		**F-E-SIG-23** Memorando enviado a los líderes de las dependencias - ARCA
2	Revisar formato base de datos	**H**	Debe identificar en la Matriz inventario de activos de información las bases de datos personales reportadas y consignar la información en el **F-E-GET-10** Reporte de bases de datos personales.	Equipo de Seguridad de la Información		Documento **F-E-GET-10** Reporte de bases de datos personales - **Consolidado**
3	Socializar gestión de bases de datos personales	**H**	Socializar la gestión de bases de datos personales con las dependencias de la Entidad.	Equipo de Seguridad de la Información Líder procesos		**F-E-SIG-05** Listado de asistencia o grabación o listado de asistencia Teams
4	Gestionar bases de datos personales	**H**	Líder del proceso debe gestionar de bases de datos personales	Enlace del Proceso		**F-E-GET-10** Reporte de bases de datos personales - **Actualizado**
5	Reportar bases de datos personales	**H**	Reportar la base de datos en el Registro nacional de bases de datos personales en la SIC.	Profesional de Seguridad		Base de datos personal registrada y actualizada en el Registro Nacional de Bases de Datos (RNBD)
6	Descargar certificado de RNBD	**A**	Descargar certificado como constancia del reporte las bases de datos **Fin de la etapa**	Profesional de Seguridad	**X**	Certificado de registro de bases de datos

5.10.1. FLUJOGRAMA "GESTIONAR RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN"

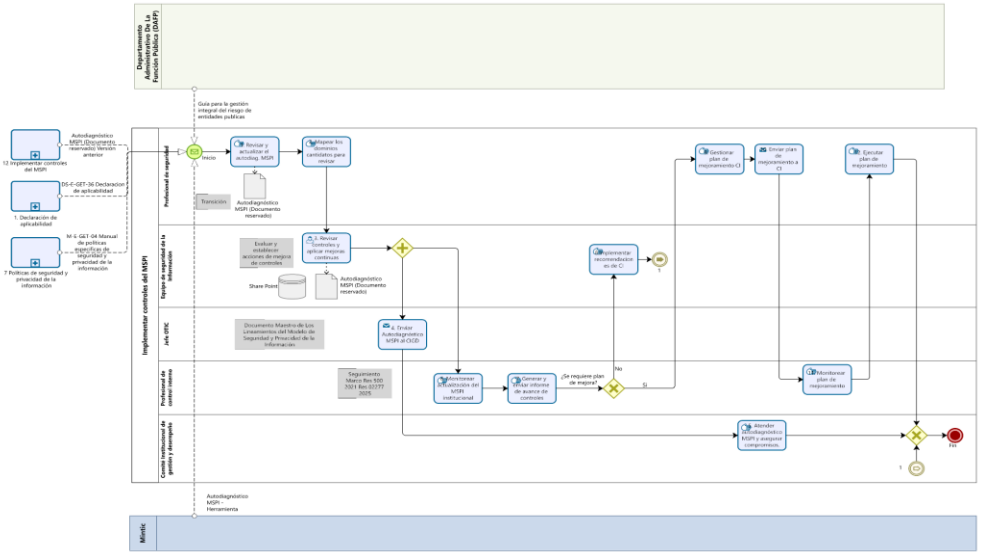


5.10.2. ACTIVIDADES "GESTIONAR RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN"

N.º.	ACTIVIDAD	CICLO PHVA	DESCRIPCIÓN	RESPONSABLE	PC	REGISTRO
1	Revisar y actualizar guía de administración del riesgo	H	Revisar y actualizar la Guía de Administración del Riesgo conforme a la Guía del DAFP, incorporando los lineamientos para la identificación, análisis, valoración y tratamiento de riesgos estratégicos, operativos, tecnológicos y de seguridad de la información, así como los mecanismos de seguimiento y reporte	Profesional de Seguridad Profesional de la OAP		Documento **G-E-SIG-05** Guía de administración del riesgo - **Actualizado**
2	Actualizar Mapa de riesgos institucional	H	Actualizar el Mapa de Riesgos Institucional, mediante la revisión, identificación, análisis, valoración y priorización de los riesgos estratégicos, operativos, tecnológicos, de seguridad de la información, legales y de corrupción, así como la actualización de controles, responsables y planes de tratamiento, garantizando su coherencia con los procesos institucionales.	Profesional de Seguridad Profesional de la OAP		Documento **F-E-SIG-28** Mapa de riesgos institucional - **Actualizado**
3	Definir cronograma de trabajo	H	Debe determinar las actividades necesarias para la identificación y valoración de riesgos	Profesional de Seguridad		Cronograma de trabajo - **Definido**

4	Enviar comunicación interna	**H**	Enviar comunicación interna a las dependencias, informando el cronograma y lineamientos para la actualización del Mapa de Riesgos Institucional, incluyendo los riesgos tecnológicos y de seguridad de la información.	Profesional de Seguridad		(Memorando o correo electrónico)
5	Socializar lineamientos para gestionar riesgos.	**H**	Debe socializar lineamientos sobre los riesgos de seguridad a los líderes de proceso.	Profesional de Seguridad		Lineamientos de riesgos - **Socializados**
6	Identificar, valorar y aprobar riesgos de seguridad	**H**	Identificar, analizar, valorar y aprobar los riesgos de seguridad de la información asociados a los procesos institucionales, mediante la realización de mesas de trabajo con los líderes y equipos de proceso, conforme a lo establecido en la **G-E-SIG-05** Guía de Administración del Riesgo.	Líder del Proceso Equipo de Seguridad de la Información		Documento **F-E-SIG-28** Mapa de riesgos institucional - **Actualizado**
7	Consolidar riesgos	**H**	Consolidar los riesgos de seguridad de la información, listo para análisis y aprobación.	Equipo de Seguridad de la Información	**X**	F-E-SIG-28 Mapa de riesgos institucional (con riesgos de seguridad) **Actualizados**
8	Enviar Mapa de riesgos consolidado	**H**	Enviar el Mapa de Riesgos Consolidado a la Oficina Asesora de Planeación (OAP) por correo electrónico	Equipo de Seguridad de la Información		Correo electrónico
9	Consolidar riegos institucionales	**H**	Consolidar todos los riesgos institucionales identificados, listos para revisión y análisis por el CIGD.	Profesional de la OAP		Documento **DS-E-SIG-25** Mapa de riesgos institucional - **Consolidado**
19	Presentar Mapa de riesgos ante el CIGD	**H**	Presentar el Mapa de Riesgos ante el Comité Institucional de Gestión del Riesgo (CIGD).	Profesional de la OAP		N/A
11	Revisar Mapa de riesgo	**A**	Revisar el Mapa de Riesgos institucional, asegurando que refleje los riesgos consolidados y preparados para aprobación. ¿Se aprueba? **Si:** Continua con la actividad 12 "Publicar riesgos institucionales" **No:** Continua con la actividad 1 " Revisar y actualizar guía de administración del riesgo"	Profesional de la OAP		Documento **F-E-SIG-25** – Acta de reunión del Comité Institucional de Gestión y Desempeño, con la Aprobación del **DS-E-SIG-25** Mapa de riesgos institucional
12	Publicar riesgos institucionales	**H**	Publicar los riesgos institucionales consolidados en la plataforma SOMOSIG, garantizando su disponibilidad y visibilidad para los usuarios autorizados **Fin de la etapa**	Profesional de la OAP	**X**	Documento **DS-E-SIG-25** Mapa de riesgos institucional - Actualizado en SOMOSIG

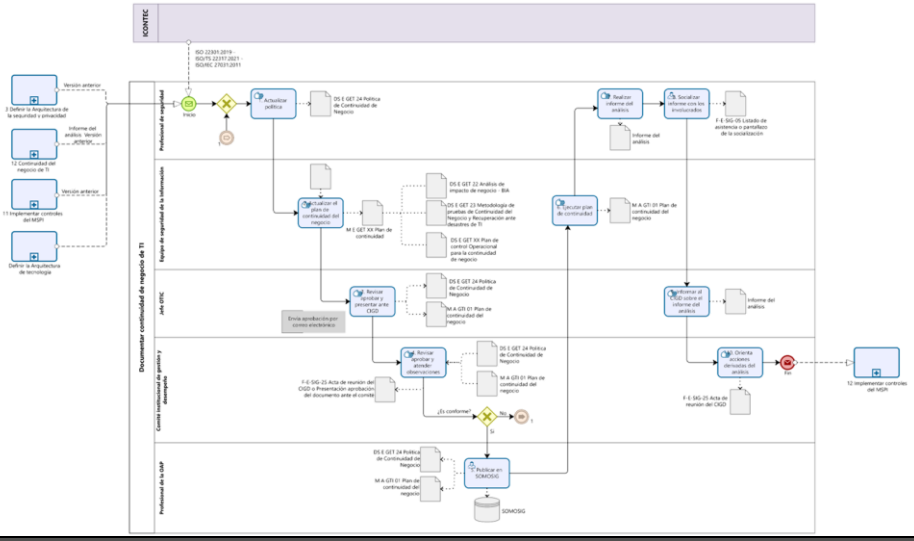
5.11.1. FLUJOGRAMA "IMPLEMENTAR CONTROLES DEL MSPI"



5.11.2. ACTIVIDADES "IMPLEMENTAR CONTROLES DEL MSPI"

N.º.	ACTIVIDAD	CICLO PHVA	DESCRIPCIÓN	RESPONSABLE	PC	REGISTRO
1	Revisar y actualizar el autodiagnóstico MSPI	**H**	Revisar y actualizar el autodiagnóstico del Modelo de Seguridad y Protección de la Información (MSPI) utilizando la herramienta del MinTIC, en concordancia con la Guía para la Gestión Integral del Riesgo de Entidades Públicas del DAFP, asegurando que refleje el estado actual de la gestión de riesgos y controles de seguridad de la información.	Profesional de Seguridad		Documento Autodiagnóstico MSPI (Documento reservado) - **Actualizado**
2	Mapear los dominios candidatos para revisar	**H**	Identificar y mapear los dominios candidatos para revisión, dejando clara su priorización y alcance para el análisis	Profesional de Seguridad		N/A
3	Revisar controles y aplicar mejoras continuas	**H**	Evaluar los controles y establecer acciones de mejora continua para optimizar su eficacia y cumplimiento de los lineamientos de seguridad y gestión de riesgos.	Equipo de Seguridad de la Información		Documento Autodiagnóstico MSPI (Documento reservado) - **Analizado**
4	Enviar Autodiagnóstico MSPI al CIGD	**H**	Remitir el autodiagnóstico MSPI al Comité Institucional de Gestión y Desempeño.	Jefe de OTIC		N/A
5	Atender autodiagnóstico MSPI y asegurar compromisos.	**A**	Conocer los resultados del autodiagnóstico MSPI, y asegurar el cumplimiento de los compromisos definidos para la mejora de la seguridad y privacidad de la información.	Comité Institucional de Gestión y Desempeño		Documento **F-E-SIG-25** – Acta de reunión del Comité Institucional de Gestión y Desempeño, con autodiagnóstico MSPI - **Actualizado**
6	Monitorear actualización del MSPI institucional	**H**	Realizar seguimiento a la actualización del Modelo de Seguridad y Privacidad de la Información (MSPI) institucional, de acuerdo con el Marco de Control Interno, la Resolución 500 de 2021 y la Resolución 2277 de 2025, asegurando cumplimiento de lineamientos, avances y compromisos en la gestión de seguridad de la información.	Profesional de Control Interno		N/A
7	Generar y enviar informe de avance de controles	**H**	Elaborar un informe detallado sobre el estado de los controles de seguridad de la información, identificando avances, hallazgos, brechas y acciones pendientes. Enviar el informe a los responsables para su revisión, análisis y retroalimentación, asegurando que sirva de base para la implementación de recomendaciones y la gestión del plan de mejoramiento de Control Interno (CI). ¿Se requiere plan de mejora? **Si:** Continua con la actividad 9 "Gestionar plan de mejoramiento CI" **No:** Continua con la actividad 8 "Implementar recomendaciones de CI"	Profesional de Control Interno	**X**	Informe de control Interno
8	Implementar recomendaciones de CI	**H**	Ejecutar las acciones derivadas de las recomendaciones del Control Interno (CI), con el fin de subsanar hallazgos..	Equipo de Seguridad de la Información		Documento Autodiagnóstico MSPI - Con evidencias de implementación de recomendaciones
9	Gestionar plan de mejoramiento CI	**H**	Plan de Mejoramiento de Control Interno (en seguridad de la información) gestionado, con acciones, responsables, plazos y evidencias documentadas	Profesional de Seguridad		Plan de Mejoramiento - **Realizado**
10	Enviar plan de mejoramiento a CI	**H**	Plan de Mejoramiento enviado a la Oficina de Control Interno, con evidencia de remisión y recepción.	Profesional de Seguridad		(Memorando o correo electrónico)
11	Monitorear plan de mejoramiento	**H**	Monitorear la ejecución del Plan de Mejoramiento	Profesional de Control Interno		Informe de control Interno - Si Aplica
12	Ejecutar plan de mejoramiento	**A**	El profesional de Seguridad de la Información ejecuta las acciones definidas en el Plan de Mejoramiento, asegurando la implementación de controles, mitigación de hallazgos y cumplimiento de los compromisos establecidos. **Fin de la etapa**	Profesional de Seguridad		Evidencias de ejecución del Plan de Mejoramiento

5.12.1. FLUJOGRAMA "DOCUMENTAR CONTINUIDAD DE NEGOCIO DE TI"



5.12.2. ACTIVIDADES "DOCUMENTAR CONTINUIDAD DE NEGOCIO DE TI"

N.º.	ACTIVIDAD	CICLO PHVA	DESCRIPCIÓN	RESPONSABLE	PC	REGISTRO
1	Actualizar política	**H**	Revisar y actualizar la Política de Continuidad de Negocio asegurando su alineación con los objetivos institucionales y la gestión de la seguridad de la información.	Profesional de Seguridad		Documento DS E GET 24 Política de Continuidad de Negocio - **Actualizado**
2	Actualizar el plan de continuidad del negocio	**H**	Actualizar el **M-A GTI-01** Plan de continuidad del negocioasegurando su alineación con la estrategia de TI La actualización incluye los documentos complementarios: **DS-E-GET-22**: Análisis de Impacto de Negocio (BIA), **DS-E-GET-23**: Metodología de Pruebas de Continuidad del Negocio y Recuperación ante Desastres de TI, Plan de Control Operacional para la Continuidad de Negocio.	Equipo de Seguridad de la Información		Documentos (**M-A GTI-01** Plan de continuidad del negocio, **DS-E-GET-22**: Análisis de Impacto de Negocio (BIA), **DS-E-GET-2**3 Metodología de Pruebas de Continuidad del Negocio y Recuperación ante Desastres de TI y Plan de Control Operacional para la Continuidad de Negocio) - **Actualizados**
3	Revisar aprobar y presentar ante CIGD	**V**	Política y Plan de Continuidad del Negocio revisados, aprobados y enviados al Comité Institucional de Gestión y Desempeño	Jefe OTIC		Documentos (**DS E GET 24** Política de Continuidad de Negocio y **M A GTI 01** Plan de continuidad del negocio) - Revisados
4	Revisar aprobar y atender observaciones	**A**	Documentos revisados y aprobados con o sin observaciones del comité, listos para implementación y socialización. ¿Es conforme? **Si:** Continua con la actividad 5 "Publicar en SOMOSIG" **No:** Continua con la actividad 1 " Actualizar política "	Comité Institucional de Gestión y Desempeño		Documento **F-E-SIG-25** – Acta de reunión del Comité Institucional de Gestión y Desempeño, con **DS E GET 24** Política de Continuidad de Negocio y **M A GTI 01** Plan de continuidad del negocio - **Aprobados**
5	Publicar en SOMOSIG	**H**	Publicar en la plataforma SOMOSIG la Política de Continuidad de Negocio y el Plan de Continuidad del Negocio, asegurando su disponibilidad y visibilidad	Profesional de la OAP	**X**	Documentos (**DS E GET 24** Política de Continuidad de Negocio y **M A GTI 01** Plan de continuidad del negocio) - **Publicados** en SOMOSIG
6	Ejecutar plan de continuidad	**H**	Implementar las acciones definidas en el **M A GTI 01** Plan de continuidad del negocio, asegurando la operatividad de los procesos críticos, la disponibilidad de recursos y la aplicación de medidas preventivas y correctivas según lo planificado.	Equipo de Seguridad de la Información		Acciones implementadas y resultados documentados
7	Realizar informe del análisis	**H**	Elaborar un informe detallado sobre los resultados del análisis realizado, para su revisión y toma de decisiones	Profesional de Seguridad		Documento - Informe del análisis
8	Socializar informe con los involucrados	**H**	Compartir y explicar el informe del análisis con las partes involucradas para su retroalimentación y seguimiento	Profesional de Seguridad		**F-E-SIG-05** Listado de asistencia o pantallazo de la socialización
9	Informar al CIGD sobre el informe del análisis	**H**	Comunicar al Comité Institucional de Gestión del Riesgo (CIGD) los resultados del informe del análisis, para su conocimiento y seguimiento	Jefe de OTIC		N/A
10	Orienta acciones derivadas del análisis	**A**	Orientar y coordinar las acciones del comité, asignando responsables, definiendo plazos y asegurando seguimiento.	Comité Institucional de Gestión y Desempeño		Acciones derivadas del análisis orientadas, con responsables, plazos y seguimiento definidos

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.