SUPERINTENDENCIA DE BANCOS
Protegemos a la Gente

MANUAL DEL PROCESO

GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

Dirección de Procesos y Mejoramiento Continuo
Versión 1.0

Enero, 2018

"LA MEJORA CONTINUA, ES EL ALIMENTO
DE LA RAZÓN Y EL CAMINO A LA EXCELENCIA"

CÓDIGO: MAN-GSI-GSI-9	**VERSIÓN:** 1.0

MANUAL DE
Gestión de Seguridad de la Información

RUBRO	NOMBRE	CARGO	FIRMA	FECHA
Elaboración:	*Ing. Gabriela Salgado*	*Experto en Administración Técnica*	Gabriela S.	12 ENE 2018
	Ing. Juan Carlos Mejía	*Asesor 5*		12 ENE. 2018
Revisión:	*Ing. Elizabeth Granda*	*Directora de Procesos y Mejoramiento Continuo*		12 ENE. 2018
Aprobación:	*Ing. Celene Vargas*	*Coordinadora General de Planificación y Mejoramiento Continuo*		12 ENE. 2018

IDENTIFICACIÓN Y TRAZABILIDAD DEL DOCUMENTO

Proceso Nivel 0:	Gestión de Planificación y Mejoramiento Continuo
Proceso Nivel 1:	Gestión de Procesos y Mejoramiento Continuo
Proceso Nivel 2:	Gestión de Seguridad de la Información
Proceso Nivel 3:	
Fecha de vigencia del documento	12 de enero del 2018
Versión del Documento:	1.0
Número de Páginas:	30
Responsable del proceso:	Director(a) de Procesos y Mejoramiento Continuo
Frecuencia de ejecución:	Mensual

REGISTRO DE VERSIONES

Versión	Descripción de la versión (motivos y cambios)	Realizado / Aprobado por	Cargo	Fecha de elaboración	Documentos que se dan de baja con la vigencia de este documento
1.0	Creación	Ana Jaramillo / Celene Vargas	Asistente Técnico / Coordinadora General de Planificación y Mejoramiento Continuo		N/A

ÍNDICE Y CONTENIDO

1. DESCRIPCIÓN DEL MANUAL GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

1.1. FICHA DEL MANUAL

Descripción:	***PROPÓSITO:*** ❖ *Determinar los esquemas de seguridad de la información que permitan a la Superintendencia de Bancos mantener la confidencialidad, disponibilidad e integridad de sus activos de información.* ***DISPARADOR:*** ❖ *Requerimientos identificados del plan estratégico institucional.* ❖ *Disposiciones de organismos externos en temas de seguridad de la información.* ❖ *Necesidades y requisitos de seguridad de la información.* ***ENTRADAS:*** ❖ *Plan Estratégico Institucional.* ❖ *Recomendaciones de auditorías de seguridad de la información.* ❖ *Análisis de riesgo de seguridad de la información.* ❖ *Resultados de la gestión de incidentes de seguridad.* ❖ *Informe de gestión de vulnerabilidades y ethical hacking.* ❖ *Memorando de estado de madurez del SGSI.* ***SUBPROCESOS:*** ❖ *Planificación de la Gestión de Seguridad de la Información.* ❖ *Implementación de la Gestión de Seguridad de la Información.* ❖ *Monitoreo y revisión de la Gestión de Seguridad de la Información.* ❖ *Mantenimiento y mejora de la Gestión Seguridad de la Información.*
Productos/Servicios del proceso:	❖ *Plan Director de Seguridad de la Información.* • *Alcance del SGSI* • *Plan de tratamiento de los riesgos con la definición de riesgos a mitigar, aceptar y/o trasladar.* • *Declaración de aplicabilidad SoA.* • *Plan de Auditorías del Sistema de Gestión de Seguridad de la Información.* • *Plan de Implementación.* • *Políticas, Metodologías de Seguridad de la Información.* • *Informe de análisis de riesgos de la Seguridad de la Información.*

	• *Acta de Constitución de proyectos.* • *Informe del cumplimiento de implementación del Plan Director de Seguridad de la Información y proyectos derivados.* • *Manuales, procedimientos, instructivos de Seguridad de la Información.* • *Informe de avances de la implementación de la documentación obligatoria y de soporte del Sistema de Gestión de Seguridad de la Información y Plan Director.* • *Sistema de Métricas del Sistema de Gestión de Seguridad de la Información.* ❖ *Levantamientos de activos y clasificación de información.* ❖ *Informes de evaluación de madurez de seguridad de información.* • *Informe de auditoría de seguridad de la información.* • *Informe de medición de desempeño del Sistema de Seguridad de la Información.* • *Informe de mejora continua (Informe de cumplimiento de lineamientos del plan de mejora).*
Responsable del proceso:	❖ *Director/a de Procesos y Mejoramiento Continuo.*
Tipo de cliente:	❖ *Interno*
Marco Legal:	❖ *Constitución de la República del Ecuador.* ❖ *Código Orgánico Integral Penal.* ❖ *Ley Orgánica de Transparencia y Acceso a la Información Pública (LOTAIP).* ❖ *Ley de Propiedad Intelectual.* ❖ *Ley de Comercio Electrónico, Firmas electrónicas y Mensajes de Datos (ley no. 2002-67).* ❖ *Estatuto Orgánico de Gestión Organizacional por procesos de la SB.* ❖ *Normas del grupo ISO: 27000.* ❖ *Normas Internas de Contraloría, otras leyes internas y externas.* ❖ *Resolución de Comité de Seguridad de la Información y Continuidad del Negocio de la SB.* ❖ *Resolución de delegaciones.*

1.2. ALCANCE DEL PROCESO

El proceso inicia con la definición de la planificación del Sistema de Gestión de Seguridad de la Información, continúa con la implementación monitoreo, revisión y concluye con la mejora continua del proceso.

1.3. NORMAS GENERALES DEL PROCESO

- El Comité de Seguridad de la Información y Continuidad del Negocio de la SB, será considerado el cuerpo rector de todo el proceso de gestión de seguridad de la información.

- El Comité de Seguridad de la Información y Continuidad del Negocio de la SB, definirá y aprobará la Política General y los objetivos estratégicos del proceso de gestión de seguridad de la información, sobre los cuales se fundamentará el Sistema de Gestión de Seguridad de la Información.

- La Dirección de Procesos y Mejoramiento Continuo definirá periódicamente (no mayor a un año) el Plan Director de Seguridad de la Información, cuyo alcance deberá estar alineado a los requerimientos y necesidades institucionales internas y externas en temas de seguridad de la información.

- El Comité de Seguridad de la Información y Continuidad del Negocio de la SB aprobará el Plan Director de Seguridad de la Información para su implementación.

- El proceso de gestión de seguridad de la información, deberá enmarcarse en directrices propuestas, normas y buenas prácticas orientadas a seguridad de la información.

- Se deberá actualizar los Planes de Seguridad en función de las conclusiones y nuevos hallazgos encontrados durante las actividades de monitoreo y revisión.

2. SUBPROCESO PLANIFICACIÓN DE LA GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

2.1. FICHA DEL SUBPROCESO

Descripción:	**PROPÓSITO:** - *Establecer la planificación para la gestión de la seguridad de la información alineada a los objetivos estratégicos, a los requerimientos y necesidades de la Superintendencia de Bancos de manera sistemática.* **DISPARADOR:** - *Disposición – requerimiento de elaboración del Plan Director de Seguridad de la Información.* **ENTRADAS:** - *Plan Estratégico Institucional.* - *Manual de Gestión de Seguridad de la Información.*

	❖ *Plan de Mejora de Seguridad de la Información*
Productos/Servicios del Subproceso:	❖ *Plan Director de Seguridad de la Información* • *Alcance del SGSI.* • *Plan de tratamiento de los riesgos con la definición de riesgos a mitigar, aceptar y/o trasladar.* • *Declaración de aplicabilidad SoA.* • *Plan de auditorías del Sistema de Gestión de Seguridad de la Información.* • *Plan de Implementación.* • *Políticas, Metodologías de Seguridad de la Información.* • *Informe de análisis de riesgos de la Seguridad de la Información.* ❖ *Levantamientos de activos y clasificación de información.*
Responsable del Subproceso:	❖ *Director(a) de Procesos y Mejoramiento Continuo*

2.2. NORMAS GENERALES DEL SUBPROCESO

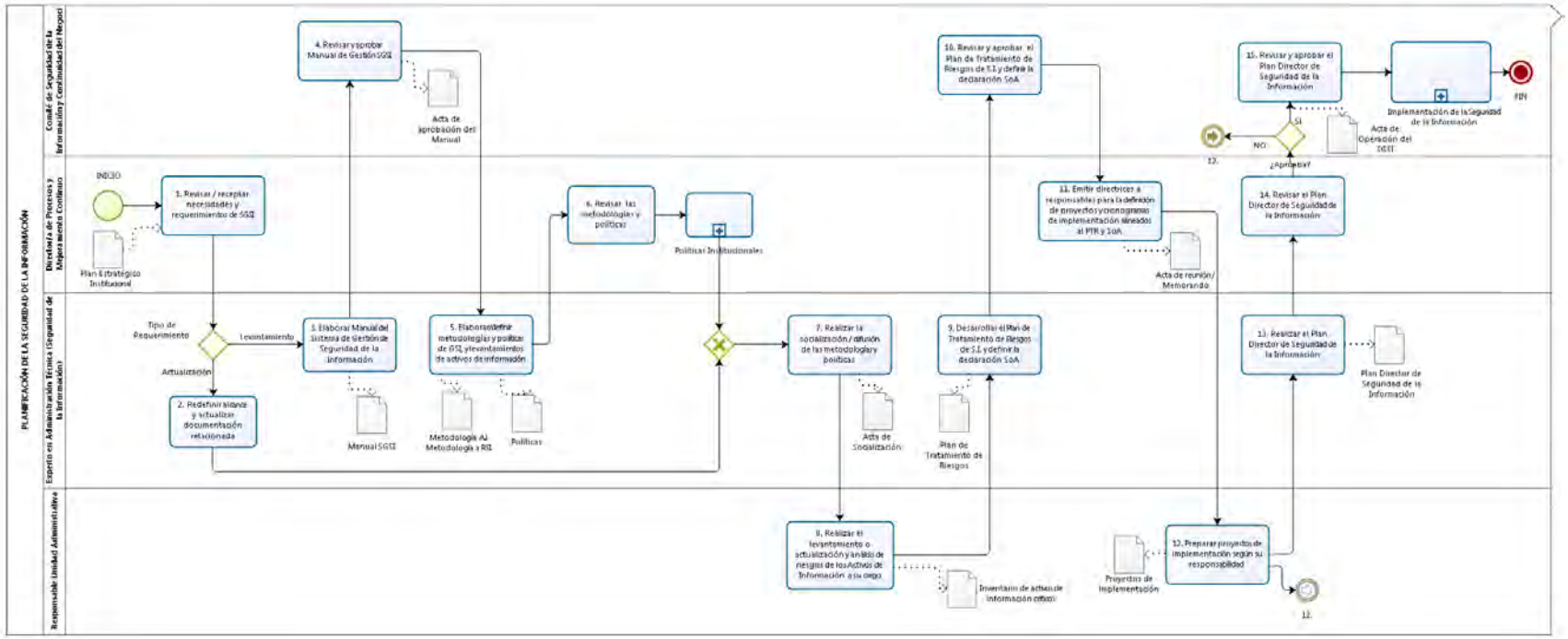
- ❖ El Comité de Seguridad de la Información y Continuidad del Negocio de la SB, define el alcance preliminar de la Seguridad de la Información, base para la planificación del proceso de gestión de seguridad de la información.

- ❖ El levantamiento y/o actualización del inventario de activos de información, es responsabilidad de los responsables del proceso con el apoyo del responsable de las actividades de Seguridad de la Información.

- ❖ El Plan Director de Seguridad de la Información deberá contener: el Plan de Tratamiento de Riesgos, la Declaración de Aplicabilidad y el plan de Implementación.

- ❖ El Plan Director de Seguridad de la Información, se define como el documento de planificación estratégica de la Seguridad de la Información cuya actualización será anual, el cual deberá alinearse al alcance y a la Planificación Estratégica de la Superintendencia de Bancos.

2.3. DIAGRAMA DE FLUJO DEL SUBPROCESO



2.4. DESCRIPCIÓN DE ACTIVIDADES

#	Actividad	Descripción	Responsable	Documentos generados
1	Revisar necesidades y requerimientos internos /externos (Sistema de Gestión de Seguridad de la Información)	Revisar e identificar los requisitos y necesidades internas y externas asociados a la Seguridad de la Información, de las unidades internas, Comité de Seguridad de la Información y Continuidad del Negocio, normativa externa, otros. **Tipo de requerimiento** **Actualización:** Pasa a la actividad 2. **Levantamiento:** Pasa a la actividad 3.	Director/a de Procesos y Mejoramiento Continuo	
2	Redefinir alcance y actualizar documentación relacionada	Se analiza los requerimientos, se redefine el alcance y documentación relacionada. Y pasa a la actividad 7.	Experto en Administración Técnica (Seguridad de la Información)	
3	Elaborar Manual del Sistema de Gestión de Seguridad de la Información	Identificar el contexto interno y externo, determinar los objetivos del Sistema de Gestión de Seguridad de la Información, compromiso de la Dirección y alineación al PEI. Definir la política general del Sistema de Gestión de Seguridad de la Información, conjuntamente con las partes relacionadas en el alcance establecido.	Experto en Administración Técnica (Seguridad de la Información)	Manual del Sistema de Gestión de Seguridad de la Información
4	Revisar y aprobar Manual de Gestión Sistema de Gestión de Seguridad de la Información	Revisar y aprobar el alcance, los objetivos, compromisos de la Dirección y política general del Sistema de Gestión de Seguridad de la Información. **¿Correcto?** **SI:** Continúa en la actividad 4 **NO:** Regresa a la actividad 2. Luego de aprobar el Manual se definen los parámetros del apetito del riesgo de SI de la SB, gestión y tratamiento y aceptación del riesgo, así como los parámetros para la tasación de activos de información crítica. Esto está establecido en el acta de aprobación.	Comité de Seguridad de la Información y Continuidad del Negocio	Acta de aprobación del Manual

5	Elaborar/definir metodologías y políticas de GSI, y levantamientos de activos de información	Elaborar y/o actualizar los documentos de metodologías para la gestión de riesgos de seguridad de la información y levantamiento de activos de información. Además se definen y elaboran las políticas.	Experto en Administración Técnica (Seguridad de la Información)	Metodologías (Activos de Información y Gestión de Riesgos de Seguridad de la Información) Políticas
6	Revisar las metodologías y políticas	Se revisa las metodologías y políticas. ¿Correctas? **SI:** Continúa en la actividad 6 **NO:** Regresa a la actividad 4	Comité de Seguridad de la Información y Continuidad del Negocio	Acta de aprobación de metodologías y políticas.
7	Realizar la socialización / difusión de las metodologías y políticas	Se efectúa la socialización de los lineamientos establecidos, metodologías y políticas, a las partes involucradas del Sistema de Gestión de Seguridad de la Información según el alcance y aplicabilidad.	Experto en Administración Técnica (Seguridad de la Información)	Acta de Socialización
8	Realizar el levantamiento o actualización y análisis de riesgos de los Activos de Información a su cargo	Luego de realizar la socialización identifica y efectúa el levantamiento de activos de información críticos a su cargo, bajo los lineamientos establecidos en la metodología de gestión de riesgos de Seguridad de la Información.	Responsable del proceso	Inventario de activos información críticos.
9	Desarrollar el Plan de Tratamiento de Riesgos de Seguridad de la Información y definir la declaración SoA	Se desarrolla el Plan de Tratamiento de Riesgos, análisis de controles implementados y formulación de la Declaración SoA, estimación de recursos, responsables y prioridades, esto se realiza conjuntamente con las Unidades Administrativas, Coordinación General de Tecnología (Encargado de seguridad informática) y demás partes relacionadas con el alcance del Sistema de Gestión de Seguridad de la Información.	Experto en Administración Técnica (Seguridad de la Información)	Plan de Tratamiento de Riesgos de Seguridad de la Información y Declaración SoA.
10	Revisar y aprobar el Plan de Tratamiento de Riesgos de S.I. y definir la declaración SoA	Se revisa el análisis de riesgos, la identificación de riesgos residuales, aceptación de riesgos, Plan de Tratamiento de Riesgos, Declaración SoA. ¿Correctos? **SI:** Se aprueban y continúa en la actividad 10.	Comité de Seguridad de la Información y Continuidad del Negocio	Acta de aprobación

		NO: Regresa a la actividad 8. Una vez aprobado se establecen las métricas de medición de la eficacia de controles o grupo de controles.		
11	Emitir directrices a responsables para la definición de proyectos y cronogramas de implementación alineados al PTR y SoA	Las directrices definen los mecanismos de operación del Sistema de Gestión de Seguridad de la Información se las define conjuntamente con las partes involucradas, se determinan responsables de definición de proyectos y cronogramas de implantación, alineados al Plan de Tratamiento de Riesgos y Declaración SoA definidos anteriormente. Se formaliza con una acta de reunión, se comunica por memorando	Experto en Administración Técnica (Seguridad de la Información)	Acta de reunión / Memorando
12	Preparar proyectos de implementación según su responsabilidad	Establecer los proyectos derivados del Plan de Tratamiento de Riesgos y Declaración SoA, se definen cronogramas, recursos necesarios, responsables conjuntamente con la Dirección Nacional de Planificación y Control de Gestión	Responsable del proceso	Acta de Constitución de Proyectos de Implementación
13	Realizar el Plan Director de Seguridad de la Información	Se realiza el Plan Director de Seguridad de la Información con la consolidación y priorización de proyectos de implementación del Sistema de Gestión de Seguridad de la Información constando principalmente de: Establecimiento de Proyectos, métricas para medición de eficacia del Sistema de Gestión de Seguridad de la Información, seguimiento de proyectos y validación de estrategias. Ejecución del GAP Análisis Establecimiento de recursos y responsables. Planes de Capacitación Plan de Auditorías Definición de Estrategias Planes de Tratamiento de Riesgos y declaración SoA.	Experto en Administración Técnica (Seguridad de la Información)	Plan Director de Seguridad de la Información.

		Clasificación y priorización de proyectos de acuerdo a: Procedencia: (normativas, cumplimiento obligatorio, análisis de riesgos y tipos de acción) y calificación por parte del Comité de Seguridad de la Información y Continuidad del Negocio: ▪ Desempeño del Sistema de Gestión de Seguridad de la Información ▪ Plan de Mejoras. Revisiones de la Dirección.		
14	Revisar el Plan Director de Seguridad de la Información	Se revisa el Plan Director de Seguridad de la Información. ¿Adecuado a necesidades y requerimientos institucionales?? **SI:** Actividad15. **NO:** Regresa a la actividad 12.	Comité de Seguridad de la Información y Continuidad del Negocio	Acta de Operación del SGSI y aprobación del PDSI
15	Revisar y aprobar el Plan Director de Seguridad de la Información	Se revisa el Plan Director de Seguridad de la Información. ¿Adecuado a necesidades y requerimientos institucionales?? **SI:** Aprueba y va al siguiente subproceso de Implementación de la Seguridad de la Información **NO:** Regresa a la actividad 12. **FIN**	Comité de Seguridad de la Información y Continuidad del Negocio	Acta de Operación del SGSI y aprobación del PDSI

3. SUBPROCESO IMPLEMENTACIÓN DEL SISTEMA DE GESTIÓN SEGURIDAD DE LA INFORMACIÓN

3.1. FICHA DEL SUBPROCESO

Descripción:	**PROPÓSITO:** ❖ *Implementar y operar el Plan Director de Seguridad de la Información en la Superintendencia de Bancos, con el fin de mitigar los posibles riesgos de seguridad de la información identificados mediante el uso de controles y proyectos de seguridad de la información.* **DISPARADOR:** ❖ *Dar cumplimiento al Plan Director de Seguridad de la Información, necesidades y requerimientos institucionales internos y externos.*

	ENTRADAS: ❖ *Plan Director de Seguridad de la Información aprobado.* ❖ *Nuevo proyectos que refieran a la seguridad de la información.*
Productos/Servicios del Subproceso:	❖ *Plan Director de Seguridad de la Información* • *Informe del cumplimiento de implementación del Plan Director de Seguridad de la Información y proyectos derivados.* • *Manuales, procedimientos, instructivos de Seguridad de la Información.* • *Informe de avances de la implementación de la documentación obligatoria y de soporte del Sistema de Gestión de Seguridad de la Información y Plan Director.* • *Sistema de Métricas del Sistema de Gestión de Seguridad de la Información.*
Responsable del Subproceso:	❖ *Director(a) de Procesos y Mejoramiento Continuo*

3.2. NORMAS GENERALES DEL PROCESO

❖ La implementación de la Seguridad de la Información, será ejecutada en base al Plan Director de Seguridad de la Información, realizado conjuntamente con las Unidades Administrativas, dentro del alcance del Sistema de Gestión de Seguridad de la Información.

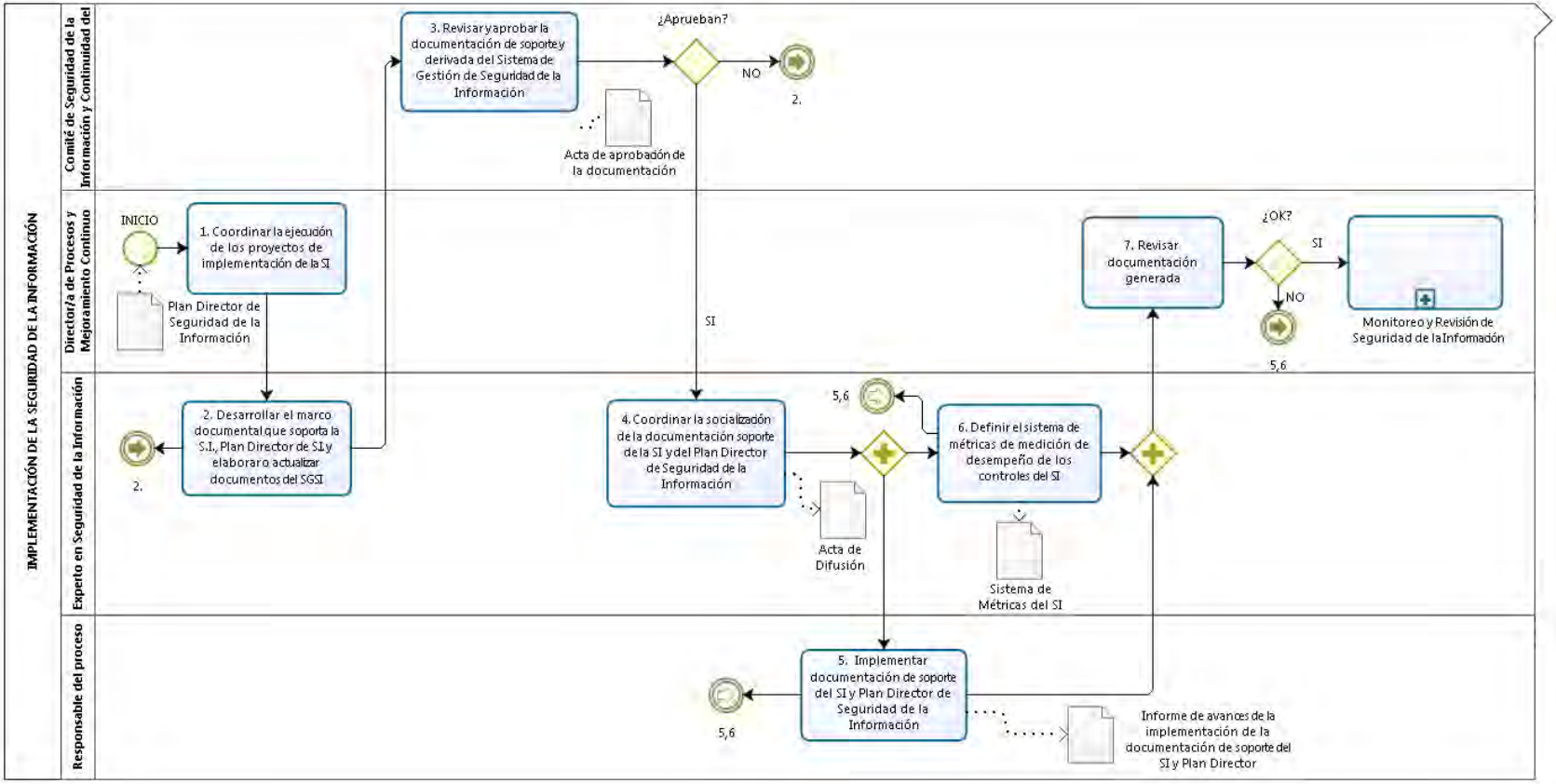
❖ Los responsables de las unidades administrativas serán los encargados de gestionar la asignación de los recursos necesarios para la implementación de la Seguridad de la Información enmarcados en sus proyectos establecidos en el Plan Director de Seguridad de la Información.

❖ Las Unidades Administrativas, deberán ajustarse a las directrices de seguridad de la información, definidas como parte de la Implementación de la Seguridad de la Información, aprobadas y socializadas en el Comité de Seguridad de la Información y Continuidad del Negocio.

❖ El experto técnico de seguridad de la información, verificará, registrará y controlará los resultados de la implementación del Plan Director de Seguridad de la Información, considerando para el efecto las actividades, dificultades, Plan de Tratamiento de Riesgos, Declaración SoA.

❖ La Coordinación General de Tecnologias de la Información y Comunicación, deberá incluir periódicamente en su Plan de Tratamiento de Riesgos de TI, el tratamiento de los riesgos identificados sobre activos de información críticos tecnológicos.

3.3. DIAGRAMA DE FLUJO DEL SUBPROCESO



3.4. DESCRIPCIÓN DE ACTIVIDADES DEL SUBPROCESO

#	Actividad	Descripción	Responsable	Documentos generados
1	Coordinar la ejecución de los proyectos de implementación de la Seguridad de la Información.	Emite las directrices de priorización para la implementación del Plan Director de Seguridad de la Información a las partes involucradas, realiza el seguimiento de los avances a dicho Plan.	Director/a de Procesos y Mejoramiento Continuo	
2	Desarrollar el marco documental que soporta la S.I., Plan Director de S.I. y elaborar o actualizar documentos del SGSI	Se desarrolla el marco documental obligatorio establecido en las normas o buenas prácticas y documentación de nivel estratégico, dicho marco documental consiste en un conjunto de directrices acerca de la documentación que se debe generar para la implementación de Seguridad de la Información. Se elabora o actualiza la documentación que se requiere o soporta la Seguridad de la Información o Plan Director de Seguridad de la Información.	Experto en Administración Técnica de seguridad de la información	Manuales, procedimientos, instructivos, etc.
3	Revisar y aprobar la documentación de soporte y derivada del Sistema de Gestión de Seguridad de la Información	Se revisa y aprueba la documentación realizada. ¿Correcta? **SI:** Se aprueban y continúa en la actividad 4 **NO:** Regresa a la actividad 2.	Comité de Seguridad de la Información y Continuidad del Negocio	Acta de aprobación de la documentación
4	Coordinar la socialización de la documentación soporte de Seguridad de la Información y del Plan Director de Seguridad de la Información.	Se socializa la documentación de soporte de la Seguridad de la Información (marco normas, manuales, procedimientos, instrucciones) y Plan Director de Seguridad de la Información, a las partes interesadas, según la aplicabilidad y el alcance de las mismas.	Experto en Administración Técnica de seguridad de la información	Acta de Difusión
5	Implementar documentación de	Implementa los proyectos derivados del Plan Director y	Responsable del proceso	Informe de avances de la

	soporte de la Seguridad de la Información y Plan Director de Seguridad de la Información	de la documentación de soporte de la Seguridad de la Información. Adicionalmente se elabora un informe de avances de la implementación.		implementación de la documentación de soporte del S.I. y Plan Director S.I.
6	Definir el sistema de métricas de medición de desempeño de los controles de la Seguridad de la Información	Se establece las métricas de medición de desempeño con las cuales se medirá el avance de implementación y efectividad de los controles de la Seguridad de la Información.	Experto en Administración Técnica de seguridad de la información	Sistema de Métricas del S.I.
7	Revisar documentación generada	Informe de avances de la implementación de la documentación de soporte del S.I., Plan Director S.I. y Sistema de Métricas del S.I. serán revisados en su totalidad, con el fin de evaluar su pertinencia. **¿OK?** **Si:** Subproceso de Monitoreo y Revisión de Seguridad de la Información **No:** Actividad 5 y 6.	Director/a de Procesos y Mejoramiento Continuo	

4. SUBPROCESO MONITOREO Y REVISIÓN DEL SISTEMA DE GESTIÓN SEGURIDAD DE LA INFORMACIÓN

4.1. FICHA DEL SUBPROCESO

Descripción:	**PROPÓSITO:** ❖ *Evaluar la Seguridad de la Información a través de auditorías que permitan determinar el desempeño y conformidad de la documentación; midiendo el grado de cumplimiento de los objetivos, planes y programas trazados en lo referente a la seguridad de la información.* **DISPARADOR:** ❖ *Cumplimiento al plan de auditorías y revisión de indicadores.* ❖ *Necesidad de análisis de madurez del sistema de gestión de seguridad de la información.* **ENTRADAS:** ❖ *Plan de Auditorías de Seguridad de la Información.* ❖ *Sistema de Métricas del Sistema de Gestión de Seguridad de la Información.*
Productos/Servicios del Subproceso:	❖ *Informes de evaluación de madurez de seguridad de información.* • *Informe de auditoría del Sistema de Seguridad de la Información.* • *Informe de medición de desempeño del Sistema de Seguridad de la Información.*
Responsable del Subproceso:	❖ *Director(a) de Procesos y Mejoramiento Continuo*

4.2. NORMAS GENERALES DEL PROCESO

❖ Anualmente se debe preparar el Plan de Auditorías de la Seguridad de la Información y debe ser una parte del Plan Director de Seguridad de la Información.

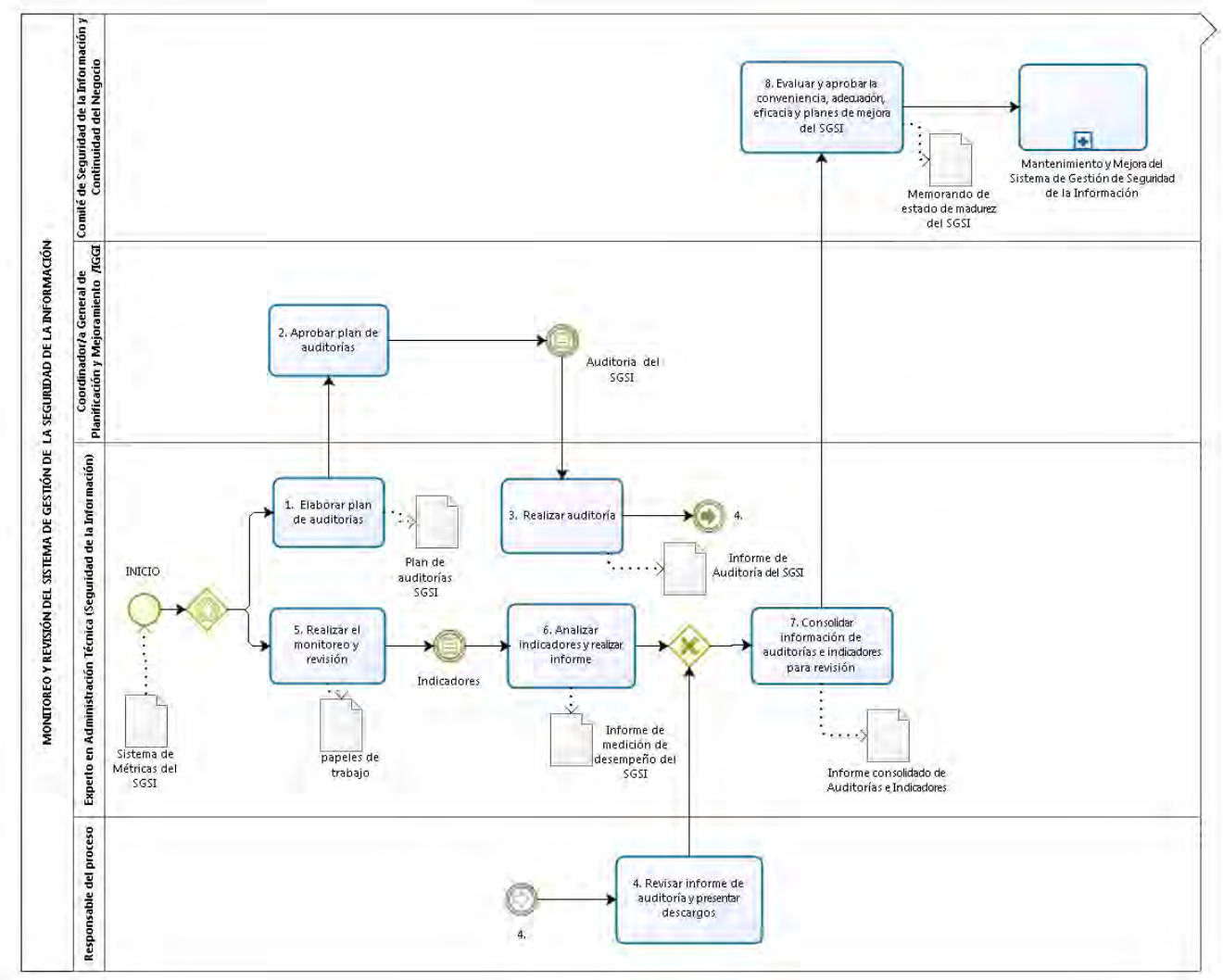
❖ Las auditorias se efectúan con base a los riesgos y amenazas determinadas en la etapa de planificación. En dicha etapa, se verifica si las brechas de seguridad de la información fueron cerradas y si los controles implementados son efectivos.

❖ Para cada proceso a auditar se debe elaborar el respectivo Plan de auditorías de la Seguridad de la Información y demás documentos de trabajo de la auditoría.

- En los casos que se generen no conformidades o reportes de mejoramiento, se debe registrar en el formato “Informe de Auditorías de la Seguridad de la Información”.

- De ser necesario, la Dirección de Procesos y Mejoramiento Continuo presenta todos los resultados y propuestas del monitoreo del sistema al Comité de Seguridad de la Información y Continuidad del Negocio.

4.3. DIAGRAMA DE FLUJO DEL SUBPROCESO



4.4. DESCRIPCIÓN DE ACTIVIDADES DEL SUBPROCESO

#	Actividad	Descripción	Responsable	Documentos generados
1	Elaborar plan de auditorías	Se verifican los hallazgos que se hayan tenido de auditorías anteriores (en el caso que hayan existido). Así también, controles, brechas o estrategias de seguridad de la información que se hayan presentado, con la finalidad de determinar la funcionalidad o estado de hallazgos.	Experto en Administración Técnica (Seguridad de la Información)	Plan de auditorías SGSI
2	Aprobar plan de auditorías	Una vez elaborado el plan, se presenta para aprobación del Coordinador/a General de Planificación y Mejoramiento Continuo e Intendente General de Gestión Institucional. De esta manera, se procede a disponer su cumplimiento al responsable.	Coordinador/a General de Planificación y Mejoramiento Continuo e Intendente General de Gestión Institucional	Memorando / correo electrónico
3	Realizar auditoría	Al iniciar la auditoría de procesos, esta comienza con la reunión de apertura, en donde se presenta el plan de auditoría, se resuelven las dudas existentes, así mismo se entrega el cronograma, directrices generales e informa las áreas a auditar. Se procede a realizar entrevistas en los diferentes puestos de trabajo de acuerdo a la lista de chequeo. El auditor realiza preguntas, solicita y revisa la documentación de soporte requerida. Examina la evidencia objetiva y registra la información esencial y/o hallazgos detectados en la auditoría. Una vez terminada la auditoría y antes de la reunión de cierre, el auditor líder y el equipo de auditores se reúnen para discutir y evaluar la evidencia objetiva hallada durante la auditoría. Analizar las No Conformidades	Experto en Administración Técnica (Seguridad de la Información)	Informe de Auditoría del Sistema de Gestión de Seguridad de la Información

		detectadas, para asegurar su validez como resultado de la auditoría. Para terminar se compila cualquier deficiencia encontrada en la auditoría se documenta registrando la No Conformidad o Conformidad, en el Informe de Auditoria.		
4	Revisar informe de hallazgos y presentar descargos	Revisa y analiza el informe de auditoría del Sistema de Gestión de Seguridad de la Información, si fuera el caso presenta los descargos respectivos en donde se aplique. Firmar la aceptación del informe de auditoría. Ir a actividad 7.	Responsable de proceso	
5	Realizar el monitoreo y revisión	Realiza el monitoreo de los errores, brechas, eventos e incidentes presentados como parte de la operación del Sistema de Gestión de Seguridad de la Información.	Experto en Administración Técnica (Seguridad de la Información)	Papeles de trabajo
6	Analizar indicadores y realizar informe	Al analizar los indicadores de los resultados de la implementación del Sistema de Gestión de Seguridad se mide considerando principalmente lo siguiente: • Si los controles efectuados fueron efectivos conforme los requisitos y necesidades establecidos de Seguridad de la Información. • Verificar el cumplimiento de las políticas y objetivos del Sistema de Gestión de Seguridad de la Información e incidentes. Realizar el seguimiento y revisión de procedimientos.	Experto en Administración Técnica (Seguridad de la Información)	Informe de medición de desempeño del Sistema de Gestión de Seguridad de la Información
7	Consolidar información de auditorías e indicadores para revisión	Se consolida la información resultante constando principalmente de lo siguiente: • Resultados de auditoría	Responsable del proceso	Informes de evaluación de madurez de seguridad de información

		y revisiones. • Retroalimentación de las partes interesadas. • Estado de acciones correctivas y preventivas. • Vulnerabilidades y amenazas no tratadas adecuadamente en la evaluación del riesgo previo. • Resultados de mediciones de eficacia. • Resultados de acciones de revisiones previas de la dirección. • Y las recomendaciones de mejora. Los cuales servirán de insumo para la revisión por parte de la dirección.		
6	Evaluar y aprobar la conveniencia, adecuación, eficacia y planes de mejora del SGSI	Se evalúa la información consolidada en el informe de evaluación de madurez de seguridad de información y demás fuentes del SGSI, tomando la decisión de: • Mejorar la eficacia del Sistema de Gestión de Seguridad de la Información • Actualización de la evaluación y plan de tratamiento de riesgos. • Modificación de procedimientos, controles, metodologías, políticas, y demás documentación de soporte del Sistema de Gestión de Seguridad de la Información. • Aprobar planes de mejoras. • Necesidades de recursos • Mejoramiento en la medición de efectividad de los controles. **Va al subproceso de Mantenimiento y Mejora del Sistema de Gestión de Seguridad de la Información**	Comité de Seguridad de la Información y Continuidad del Negocio	Memorando de estado de madurez del Sistema de Gestión de Seguridad de la Información

5. SUBPROCESO MANTENIMIENTO Y MEJORA DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

5.1. FICHA DEL SUBPROCESO

Descripción:	**PROPÓSITO:** ❖ *Mantener y mejorar constantemente la eficacia del Sistema de Gestión de Seguridad de la Información, conforme la implementación de la política, objetivos estratégicos, auditorías, análisis de los eventos monitorizados, mediante la implementación de las acciones correctivas o preventivas.* **DISPARADOR:** ❖ *Cumplimiento de acciones correctivas contempladas en el informe de auditorías y de desempeño del Sistema de Gestión de Seguridad de la Información* **ENTRADAS:** ❖ *Informes de evaluación de madurez de seguridad de información.*
Productos/Servicios del Subproceso:	○ *Informe de cumplimiento de lineamientos del plan de mejora.*
Responsable del Subproceso:	❖ *Director(a) de Procesos y Mejoramiento Continuo*

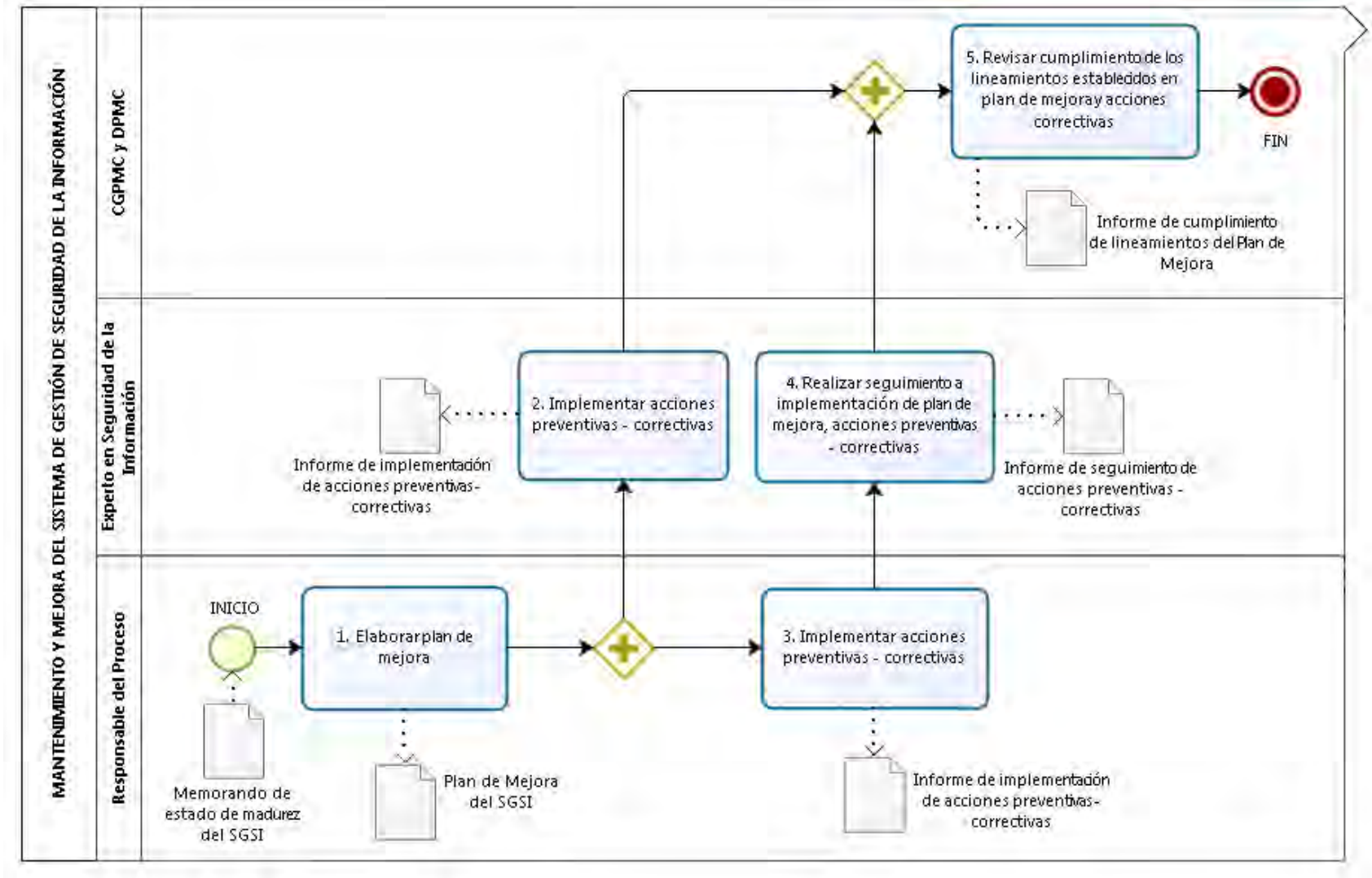
5.2. NORMAS GENERALES DEL PROCESO

❖ Cada unidad administrativa responsable del proceso, debe elaborar el plan de mejora solicitado por la DPMC.

❖ El experto en administración técnica de seguridad de la información debe registrar, monitorear y dar seguimiento a los planes de acción y/o hallazgos levantados como parte del Plan de Mejora del Sistema de Gestión de Seguridad de la información.

❖ La Dirección de Procesos y Mejoramiento Continuo en conjunto con los responsables de los procesos, deberán establecer los compromisos en el Plan de Mejora, considerando los responsables y plazos.

5.3. DIAGRAMA DE FLUJO DEL SUBPROCESO



5.4. DESCRIPCIÓN DE ACTIVIDADES DEL SUBPROCESO

#	Actividad	Descripción	Responsable	Documentos generados
1	Elaborar plan de mejora	Elabora el plan de mejoras con el asesoramiento del Experto en Administración Técnica en el cual se identifica y determina las oportunidades de mejora y las no conformidades de la operación y/o implementación. Se evalúan las acciones para evitar la ocurrencia de no conformidades o que las identificadas previamente no se vuelvan a evidenciar. Se identifican las acciones necesarias para evitar que una oportunidad de mejora no se manifieste en una no conformidad.	Responsable del proceso	Plan de Mejora del Sistema de Gestión de Seguridad de la Información
2	Implementar acciones preventivas - correctivas	Implementa las acciones preventivas o correctivas estratégicas necesarias, se registran los resultados de las acciones tomadas y se envía un informe al Comité de Seguridad de la Información y Continuidad del Negocio para su seguimiento. **Ir a actividad 5.**	Experto en Administración Técnica de seguridad de la información	Informe de implementación de acciones preventivas - correctivas
3	Implementar acciones preventivas - correctivas	Implementa las acciones preventivas o correctivas dentro de su ámbito de aplicación, se registran los resultados de las acciones tomadas y se remite un informe de avance al experto de seguridad de la información para su seguimiento.	Responsable del proceso	Informe de implementación de acciones preventivas - correctivas
4	Realizar seguimiento a implementación de plan de mejora, acciones preventivas - correctivas	Revisa las acciones preventivas y correctivas tomadas, para lo cual se debe identificar las evidencias objetivas que aseguren que las acciones han sido eficaces. Y esto se consolida en un informe de seguimiento el cual es remitido al Comité de Seguridad de la Información y Continuidad del Negocio.	Experto en Administración Técnica	Informe de seguimiento de acciones preventivas - correctivas
5	Revisar cumplimiento	Evalúan el informe de seguimiento de la implantación	Coordinador/a General de	Informe de mejora continua - Informe

	de los lineamientos establecidos en plan de mejora y acciones correctivas	eficaz de las acciones preventivas y/o correctivas por parte de las unidades responsables del proceso, con el propósito del mejoramiento continuo del Sistema de Gestión de Seguridad de la Información. Se formaliza mediante un acta de reunión. **FIN**	Planificación y Mejoramiento Continuo y Director/a de Procesos y Mejoramiento Continuo	de cumplimiento de lineamientos del Plan de Mejora

6. INDICADORES DE GESTIÓN DEL PROCESO

Los indicadores se encuentran descritos como anexos en el formato F-GSI-01 - Fichas de Indicadores de Procesos.

7. TÉRMINOS Y DEFINICIONES

Activo de información (AI).- como parte del Sistema de Gestión de Seguridad de la Información, se refiere a cualquier información o elemento relacionado con la gestión o tratamiento de la misma pudiendo ser: sistemas, soportes, edificios, personas, etc., con valor para la institución.

Bitácora.- es un registro de las acciones, efectuadas en un trabajo, tarea o actividad, la cual incluirá los sucesos que tuvieron lugar, las fallas que se produjeron, los cambios y los costos ocasionados.

CID.- acrónimo español de confidencialidad, integridad y disponibilidad, las dimensiones básicas de la seguridad de la información.

CSIyCN.- Comité de Seguridad de la Información y Continuidad del Negocio de la SB

Compromiso de la Dirección.- lineamiento firme de la Dirección de la organización con el establecimiento, implementación, operación, monitorización, revisión, mantenimiento y mejora del Sistema de Gestión de Seguridad de la Información. La versión de 2013 de ISO 27001 lo engloba bajo la cláusula de Liderazgo.

Declaración SoA (Declaración de Aplicabilidad).- Documento que enumera los controles aplicados por el Sistema de Gestión de Seguridad de la Información de la organización -tras el resultado de los procesos de evaluación y tratamiento de riesgos- y su justificación, así como la justificación de las exclusiones de controles del anexo A de ISO 27001.

Estándares.- Conjunto de parámetros técnicos, de seguridad, a configurar en cada uno de los distintos componentes de tecnología.

Gestión de incidentes de seguridad de la información.- Procesos para detectar, reportar, evaluar, responder, tratar y aprender de los incidentes de seguridad de la información.

Gestión de Riesgos de Seguridad de la Información (GRSI).- Actividades coordinadas para dirigir y controlar los riesgos asociados a los Activos de Información críticos de la Organización.

Gestión de riesgos.- Actividades coordinadas para dirigir y controlar una organización con respecto al riesgo. Se compone de la evaluación y el tratamiento de riesgos

Inventario de activos.- Lista de todos aquellos recursos (físicos, de información, software, documentos, servicios, personas, intangibles, etc.) dentro del alcance del Sistema de Gestión de Seguridad de la Información, que tengan valor para la organización y necesiten por tanto ser protegidos de potenciales riesgos.

Normas.- Definiciones concretas sobre cada uno de los temas de seguridad de la información para las distintas tareas que se desarrollan en la SBS.

Plan de Tratamiento de Riesgos.- Identifica las acciones, recursos, responsabilidades y prioridades en la gestión de los riesgos de seguridad de la información.

Política General.- Conjunto de principios generales, que soportan la gestión de la seguridad de la información en concordancia con los requerimientos institucionales, leyes, regulaciones.

Procedimientos.- Contienen un detalle de actividades o acciones a seguir por el personal, ante distintas situaciones que surgen de actividades operativas.

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.

SGSI.- Sistema de Gestión de Seguridad de la Información.

Vulnerabilidad.- Debilidad de un activo o control que puede ser explotada por una o más amenazas.

8. LISTADO DE DOCUMENTO Y ANEXOS

8.1. DOCUMENTOS

Código	Nombre del documento	Ubicación Física	Ubicación Digital
N/A	Manual del Sistema de Gestión de Seguridad de la Información	N/A	N/A
N/A	Acta de aprobación del Manual	N/A	N/A
N/A	Metodologías (Activos de Información y Gestión de Riesgos de Seguridad de la Información)	N/A	N/A
N/A	Políticas	N/A	N/A
N/A	Acta de aprobación de metodologías y políticas.	N/A	N/A
N/A	Acta Socialización	N/A	N/A
N/A	Inventario de activos información críticos.	N/A	N/A
N/A	Plan de Tratamiento de Riesgos de Seguridad de la Información	N/A	N/A
N/A	Declaración SoA.	N/A	N/A
N/A	Acta de Constitución de Proyectos de Implementación	N/A	N/A
N/A	Plan Director de Seguridad de la Información.	N/A	N/A
N/A	Acta de Operación del SGSI y aprobación del PDSI	N/A	N/A
N/A	Manuales, procedimientos, instructivos, etc.	N/A	N/A
N/A	Acta de aprobación de la documentación	N/A	N/A
N/A	Acta de Difusión	N/A	N/A
N/A	Informe de avances de la implementación de la documentación de soporte del S.I. y Plan Director S.I.	N/A	N/A
N/A	Sistema de Métricas del S.I.	N/A	N/A
N/A	Informe de medición de desempeño del Sistema de Gestión de Seguridad de la Información	N/A	N/A
N/A	Informe de Auditoría del Sistema de Gestión de Seguridad de la Información	N/A	N/A
N/A	Informes de evaluación de madurez de seguridad de información	N/A	N/A
N/A	Memorando de estado de	N/A	N/A

	madurez del Sistema de Gestión de Seguridad de la Información		
N/A	Plan de Mejora del Sistema de Gestión de Seguridad de la Información	N/A	N/A
N/A	Informe de implementación de acciones preventivas - correctivas	N/A	N/A
N/A	Informe de seguimiento de acciones preventivas - correctivas	N/A	N/A
N/A	Informe de mejora continua - Informe de cumplimiento de lineamientos del Plan de Mejora	N/A	N/A

8.2. ANEXOS

Anexo 1 Ficha de Indicadores de Gestión de Procesos – Gestión de Seguridad de la Información - F-GSI-01