SUPERINTENDENCIA DE BANCOS
Protegemos a la Gente

MANUAL DEL PROCESO

GESTIÓN DE SEGURIDAD INFORMÁTICA

Dirección de Gobernanza de TI e Innovación
Versión 1.0
Noviembre, 2017

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

CÓDIGO:MAN-GTI-GSI-13	**VERSIÓN:**1.0

MANUAL DE

Gestión de Seguridad Informática

RUBRO	NOMBRE	CARGO	FIRMA	FECHA
Elaboración:	*Lic. Benjamín Nicolalde*	*Experto en Administración Técnica 2*		26 DIC. 2017
Revisión:	*Ing. Elizabeth Granda*	*Directora de Procesos y Mejoramiento Continuo*		26 DIC. 2017
	Ing. Edison Auz	*Director de Gobernanza de TI e Innovación*		26 DIC. 2017
	Ing. Nelson Quintana	*Coordinador General de Tecnologías de Información y Comunicación*		26 DIC. 2017
Aprobación:	*Ing. Celene Vargas*	*Coordinadora General de Planificación y Mejoramiento Continuo*		26 DIC. 2017

IDENTIFICACIÓN Y TRAZABILIDAD DEL DOCUMENTO

Proceso Nivel 0:	Gestión de Tecnologías de Información y Comunicación (TIC)
Proceso Nivel 1:	Gestión de Gobernanza de TI e Innovación
Proceso Nivel 2:	Gestión de Seguridad Informática
Proceso Nivel 3:	n/a
Versión del Documento:	1.0
Número de Páginas:	26
Responsable del proceso:	Director de Gobernanza de TI e Innovación
Frecuencia de ejecución:	Continua

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	Lic. Benjamín Nicolalde / Ing.Celene Vargas	Experto en Administración Técnica 2 / Coordinadora General de Planificación y Mejoramiento Continuo		

ÍNDICE Y CONTENIDO

1. DESCRIPCIÓN DEL MANUAL DEL PROCESO DE GESTIÓN DE SEGURIDAD INFORMÁTICA

1.1. FICHA DEL MANUAL

Descripción:	**PROPÓSITO:** ❖ *Proteger la integridad y privacidad de la información almacenada y procesada por la infraestructura tecnológica institucional que soportan los procesos de supervisión y administrativos internos, administrando los riesgos tecnológicos, creando controles, procesos, procedimientos, políticas y reglamentos que permitan asegurar la confidencialidad, disponibilidad e integridad de la información.* **DISPARADOR:** ❖ *Necesidad de aplicar controles de seguridad informática determinados en el Plan Director de Seguridad de la Información y producto de la incorporación o cambios en los componentes de la infraestructura tecnológica institucional.* ❖ *Necesidad de mantener una plataforma tecnológica que opere bajo niveles aceptables de seguridad y permita mantener confidencialidad, disponibilidad e integridad de la información.* ❖ *Necesidad de cumplir requerimientos establecidos por organismos de control.* **ENTRADAS:** ❖ *Plan Director de Seguridad de la Información.* ❖ *Reportes de análisis de monitoreo de la plataforma, eventos o incidentes detectados.* ❖ *Análisis ethical hacking.* ❖ *Leyes, reglamentos, normas.* ❖ *Plan Anual de Contratación de la SB (PAC).* **SUBPROCESOS***:* ❖ *Planificación de Controles de Seguridad Informática.* ❖ *Implementación del Plan de Seguridad Informática.* ❖ *Monitoreo de la Implementación del Plan de Seguridad Informática.*
Productos/Servicios del proceso:	❖ *Plan de Seguridad Informática.* ❖ *Políticas, estándares y marcos de referencia para el gobierno de TI.* ❖ *Informes de ejecución del Aseguramiento de Calidad y Seguridad Informática.*
Responsable del	❖ *Director/a de Gobernanza de TI e Innovación.*

proceso:	
Tipo de cliente:	❖ *Cliente interno.*
Marco Legal:	❖ *Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos.* ❖ *Ley Orgánica del Sistema Nacional de Contratación Pública.* ❖ *Normas de Control Interno de la Contraloría General del Estado.* ❖ *Reglamento de adquisición de software del Código Ingenios.* *Marcos y estándares de referencia:* ❖ *Normas ISO familia 27000, Seguridad de la Información* ❖ *COBIT Gobierno de TI.* ❖ *ITIL Gestión de Servicios de Tecnología.*

1.2. ALCANCE DEL PROCESO DE GESTIÓN DE SEGURIDAD INFORMÁTICA

El proceso de gestión de la seguridad informática comprende la implementación de controles definidos en el Plan Director de Seguridad de la Información sobre los componentes de la infraestructura tecnológica institucional y otras necesidades que permitan mantener la operación normal y segura de los servicios informáticos institucionales y finaliza con el monitoreo, que permite establecer la correcta y eficiente operación de los controles implementados.

1.3. NORMAS GENERALES DEL PROCESO DE GESTIÓN DE SEGURIDAD INFORMÁTICA

- Las políticas de seguridad informática son de aplicación obligatoria para todos los funcionarios de la institución.

- El Plan Director de Seguridad de la Información priorizará controles generales aplicados a los activos de la información almacenados o procesados por medios tecnológicos, para los que se deberán definir controles técnicos a implementarse en la infraestructura tecnológica y servicios informáticos institucionales.

- La implementación de controles informáticos deberá someterse a un proceso de monitoreo previa su aprobación y salida a producción.

- La definición de controles técnicos se efectuará tomando como base la aplicación de estándares, marcos legales y normativos.

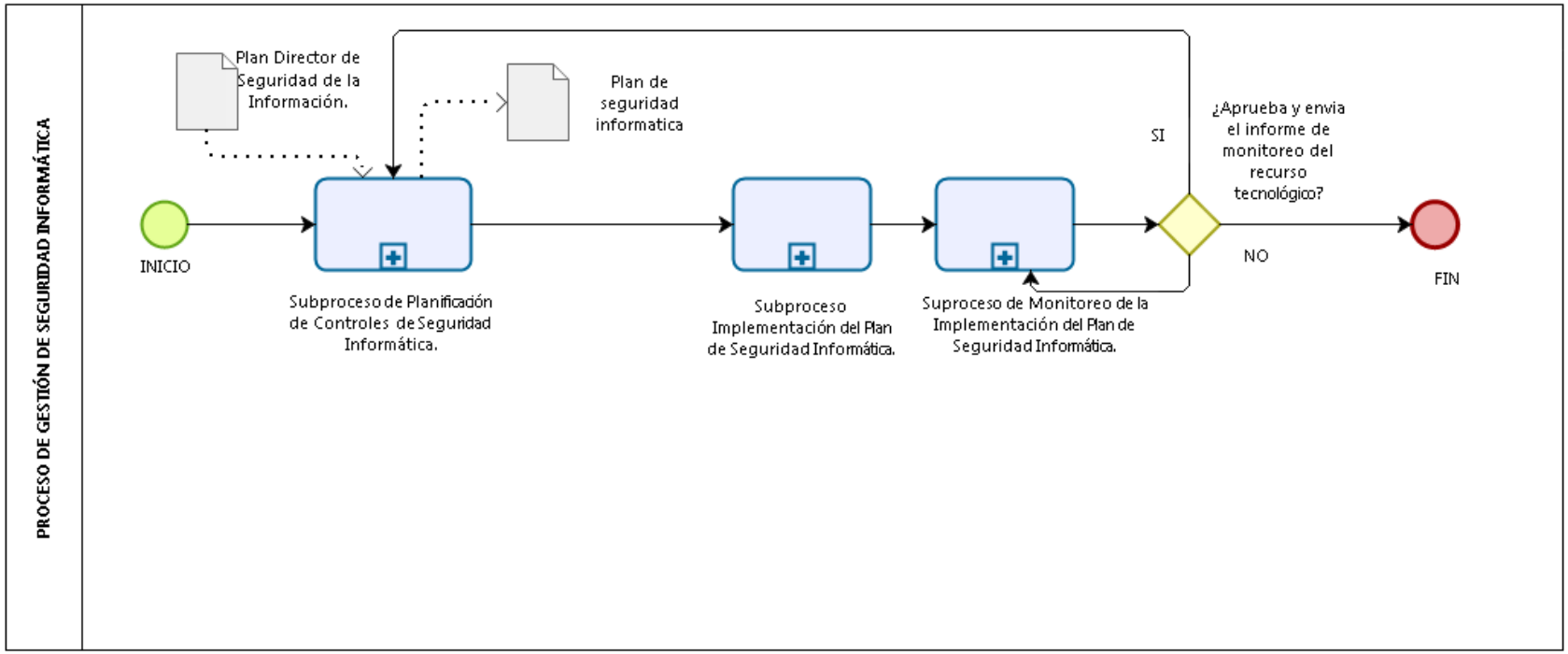
- Se aplicará el criterio del mínimo privilegio en la aplicación de controles informáticos, dependiendo de la necesidad de acceso, de acuerdo a los criterios de disponibilidad, confidencialidad e integridad.

- Todo control de seguridad informática implementado, deberá someterse a un proceso de monitoreo que permita establecer su adecuada operación.

- Los informes de monitoreo de controles informáticos implementados que contengan novedades relacionadas con su aplicación efectiva, deberán ser canalizados para la revisión por el Subproceso del Planificación de Controles de Seguridad Informática.

- La información generada por el monitoreo de los controles informáticos implementados, deberá alimentar la base de conocimiento de monitoreo, efectuado por el responsable del Equipo de Gestión de Seguridad Informática.

2. DIAGRAMA DE FLUJO DEL PROCESO DE GESTIÓN DE SEGURIDAD INFORMÁTICA.



3. DESCRIPCIÓN DEL SUBPROCESO PLANIFICACIÓN DE CONTROLES DE SEGURIDAD INFORMÁTICA

3.1. FICHA DEL SUBPROCESO

Descripción:	**DISPARADOR:** ❖ *Necesidad de mantener una plataforma tecnológica que opere bajo niveles aceptables de seguridad y permita mantener la confidencialidad, disponibilidad e integridad de los activos de información almacenados y procesados por medios tecnológicos, así también como identificar oportunamente las amenazas y debilidades de la infraestructura y procesos de la gestión tecnológica.* **ENTRADAS:** ❖ *Plan Director de seguridad de la información.* ❖ *Plan de implementación de Control de Seguridad Informática histórico.* ❖ *Informes del Plan de Tratamiento de Riesgos Tecnológicos.* ❖ *Reportes de auditoría y riesgos tecnológicos.* ❖ *Eventos o incidentes de seguridad informática.* ❖ *Análisis ethical hacking.* ❖ *Leyes, reglamentos y normas.* ❖ *Plan de Tratamiento de Riesgos Tecnológicos* ❖ *Eventos e incidentes de seguridad informática.*
Productos/Servicios del proceso:	❖ *Plan de seguridad informática.*

3.2. NORMAS ESPECÍFICAS DEL SUBPROCESO PLANIFICACIÓN DE CONTROLES DE SEGURIDAD INFORMÁTICA.

- La planificación de controles de seguridad informática definirá controles técnicos a implementarse en la infraestructura tecnológica y servicios informáticos institucionales, según requerimientos establecidos por el Plan Director de Seguridad de la Información, el plan de seguridad informática histórico, reportes de análisis de monitoreo de la plataforma, análisis ethical hacking, leyes, reglamentos, normas, eventos e incidentes de seguridad informática.

- La definición de controles técnicos se efectuará tomando como base la aplicación de estándares, marcos legales y normativos.

- Se aplicará el criterio del mínimo privilegio en la aplicación de controles informáticos.

- El Equipo de Gestión de Seguridad Informática será conformado por un Líder de Equipo de la Dirección de Gobernanza de TI e Innovación y al menos un técnico de cada unidad de la Coordinación General de Tecnologías de Información y Comunicación con conocimientos afines al control a implementar.

- La formalización de los equipos de trabajo se efectuará mediante la suscripción del acta de constitución del proyecto u orden de trabajo (incluyendo el cronograma de actividades), dependiendo de la complejidad del control a implementar, será suscrita por el Director de Gobernanza de TI e Innovación y el Coordinación General de Tecnologías de Información y Comunicación.

- La definición de controles de seguridad informática deberá efectuarse mediante el análisis de alternativas tecnológicas que permitan evaluar y seleccionar las que más se ajusten a las necesidades institucionales.

- El seguimiento de la implementación de los controles de seguridad informática, dependiendo de la complejidad de implementación, se efectuará mediante los instrumentos de gestión de proyectos tecnológicos o el cronograma respectivo de implementación.

- La periodicidad de la actualización del Plan de Implementación de Controles de Seguridad Informática dependerá de la frecuencia con que se reciban los disparadores del proceso y cada vez que el Subproceso de Monitoreo de la Implementación del Plan de Seguridad Informática emita informes de incidencias.

- La socialización del Plan de Implementación de Controles de Seguridad Informática y sus actualizaciones, se efectuará formalmente mediante memorando interno, la información se publicará en el Sistema Documental Alfresco.

- El Coordinador General de Tecnologías de Información y Comunicación será responsable de la aprobación del Plan de Implementación de Controles de Seguridad Informática.

- El Plan de Tratamiento de Riesgos Tecnológicos definirá controles ISO para los componentes informáticos asociados a cada control informático requerido por el Plan Director de Seguridad de la Información.

- El Equipo de Gestión de Riesgos Tecnológicos será conformado por un Líder de Equipo de la Dirección de gobernanza de TI e Innovación y al menos un técnico de cada unidad de la Coordinación General de Tecnologías de Información y Comunicación con conocimientos afines al control analizado.

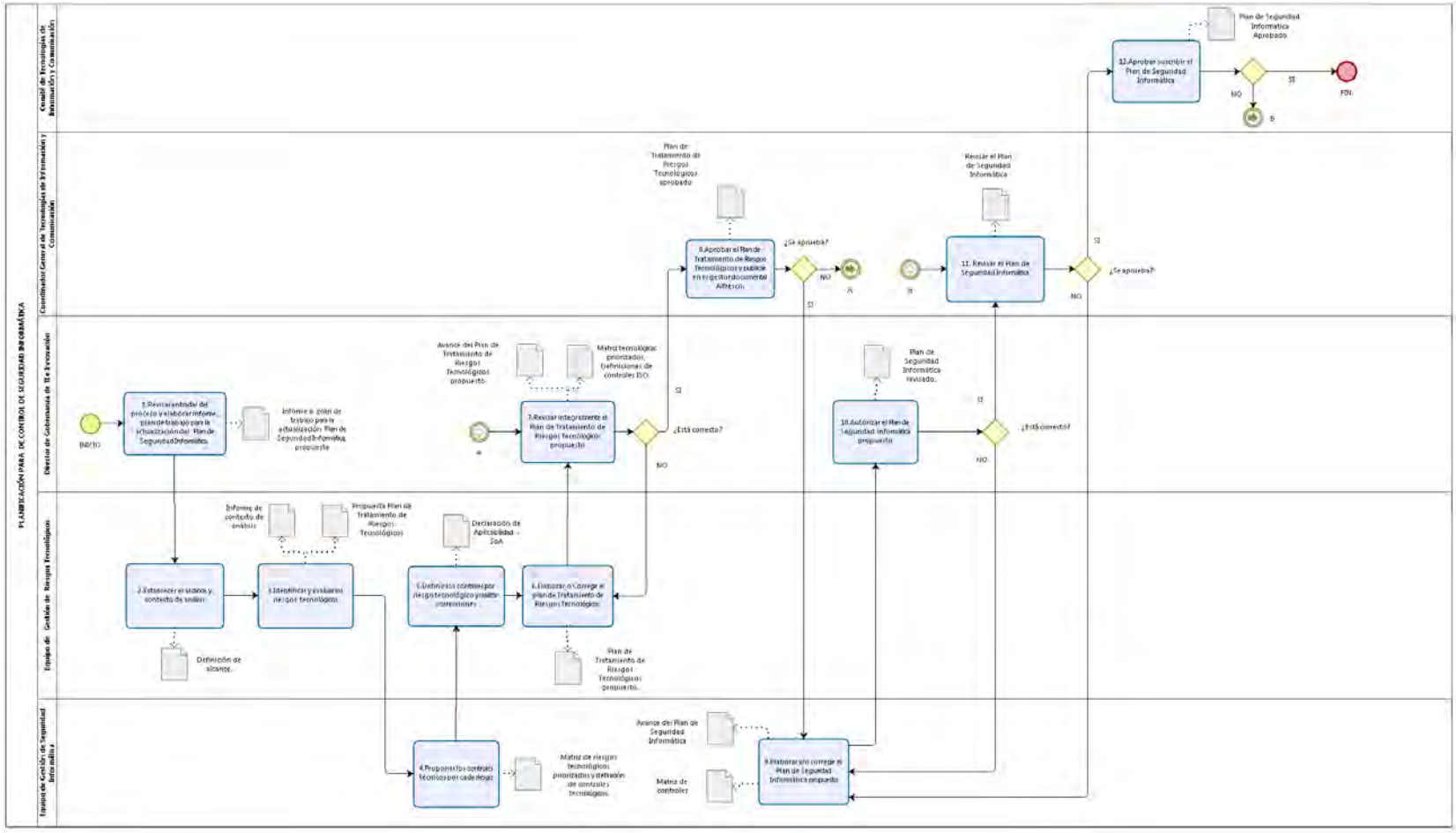
- La formalización de los equipos de trabajo se efectuará mediante acta suscrita por el Coordinador de General de Tecnologías de Información y Comunicación, el Director de Gobernanza de TI e Innovación y el Director de Soluciones Tecnológicas y/o el Director de Infraestructura y Operaciones, según la proveniencia de los recursos involucrados.

- El seguimiento para la ejecución del proceso se efectuará mediante el cronograma respectivo.

- La periodicidad de la actualización del Plan de Tratamiento de Riesgos Tecnológicos dependerá de la frecuencia con que se reciban los disparadores del proceso.

- El Plan de Tratamiento de Riesgos Tecnológicos y sus actualizaciones, será aprobado por el Coordinador General de Tecnologías de la Información y Comunicación.

3.3. DIAGRAMA DE FLUJO DEL SUBPROCESO PLANIFICACIÓN PARA DE CONTROLES DE SEGURIDAD INFORMÁTICA.



3.4. DESCRIPCIÓN DE ACTIVIDADES DEL SUBPROCESO PLANIFICACIÓN DE CONTROLES DE SEGURIDAD INFORMÁTICA.

#	Actividad	Descripción	Responsable	Documentos generados
1	Revisar entradas del proceso y elaborar informe , plan de trabajo para la actualización del Plan de Seguridad Informática	Se revisará de manera detallada la documentación que sustenta el inicio de la gestión o actualización del Plan de Seguridad Informática, la documentación inicial a considerar para esta actividad es el Plan Director de Seguridad de la Información, plan de seguridad informática histórico, reportes de análisis de monitoreo de la plataforma, análisis ethical hacking, leyes, reglamentos, normas, eventos e incidentes de seguridad informática. Se definirá el equipo de trabajo para revisar los requerimientos y plan de trabajo. En esta epata se debe estipular las estrategias para la implementación, recursos a ser usados(tecnológicos y no tecnológicos), cronogramas	Director de Gobernanza de TI e Innovación	Informe y plan de trabajo para la actualización Plan de Seguridad Informática, propuesta.
2	Establecer el alcance. y contexto de análisis	Se analizará los aspectos internos y externos a fin de determinar el alcance y las limitaciones existentes para la gestión del Plan de Tratamiento de Riesgos Tecnológicos.	Equipo de Gestión de Riesgos Tecnológicos	Definición de alcance.
3	Identificar y evaluar los riesgos tecnológicos	Se efectuará el reconocimiento y análisis de los elementos activos de información tecnológica crítica, amenazas, vulnerabilidades, controles existentes, consecuencias, entre otros, midiendo el impacto y la probabilidad de ocurrencia de cada problema de TI en los servicios de la institución para el cálculo o	Equipo de Gestión de Riesgos Tecnológicos	Informe de contexto de análisis, Propuesta Plan de Tratamiento de Riesgos Tecnológicos

#	Actividad	Descripción	Responsable	Documentos generados
		evaluación del impacto; se incluirá las consecuencias y la priorización del tratamiento de los riesgos.		
4	Proponer los controles técnicos por cada riesgo	Definir controles técnicos por componente tecnológico para cada riesgo incluido en el informe de tratamiento de riesgos tecnológicos, de tal forma que permitan atender la recomendación de implementación de controles tecnológicos emitidos por el Plan Director de Seguridad de la Información.	Equipo de Gestión de Seguridad Informática	Matriz de riesgos tecnológicos priorizados y definición de controles tecnológicos.
5	Definir los controles por riesgo tecnológico y realizar correcciones	Se definirá y priorizará los controles ISO que permitan gestionar cada riesgo	Equipo de Gestión de Riesgos Tecnológicos	Declaración de Aplicabilidad – SoA
6	Elaborar o Corregir el plan de Tratamiento de Riesgos Tecnológicos	Elaborar el plan de Tratamiento de Riesgos Tecnológicos, con los controles establecidos y proyectos de implementación de los mismos.	Equipo de Gestión de Riesgos Tecnológicos	Plan de Tratamiento de Riesgos Tecnológicos propuesto.
7	Revisar integralmente el Plan de Tratamiento de Riesgos Tecnológicos propuesto	Se realizar el Tratamiento de Riesgos Tecnológicos desarrollado por el Equipo de Gestión de Riesgos Tecnológicos. ¿Está correcto? **SI:** Actividad 6 **NO:** Actividad 8	Director de Gobernanza de TI e Innovación	Avance del Plan de Tratamiento de Riesgos Tecnológicos propuesto, Matriz tecnológicas priorizados, Definiciones de controles ISO
8	Aprobar el Plan de Tratamiento de Riesgos Tecnológicos y publicar en el gestor documental Alfresco.	Se aprobará el Plan de Tratamiento de Riesgos Tecnológicos. Una vez que esté aprobado se entrega la matriz de riesgos actualizada al equipo de seguridad informática y se publica en el gestor documental Alfresco. ¿Se aprueba? **SI:** Actividad 9 **NO:** Actividad 7	Coordinador General de Tecnologías de Información y Comunicación	Plan de Tratamiento de Riesgos Tecnológicos aprobado
9	Elaborar y/o	El Equipo de Gestión de	Equipo de	Avance del Plan de

#	Actividad	Descripción	Responsable	Documentos generados
	corregir el Plan de Seguridad Informática propuesto	Seguridad Informática elabora el Plan de Seguridad Informática, tomando como insumo el Plan de Tratamiento de Riesgo Tecnológicos aprobado, adicionalmente en este plan se debe definir y actualizar las políticas (específicas, operativas, entre otras.)objetivos y alcance de la seguridad informática	Gestión de Seguridad Informática	Seguridad Informática, matriz de controles
10	Autorizar el Plan de Seguridad informática propuesto	Se autorizará el Plan de Seguridad Informática propuesto. ¿Está correcto? **SI:** Actividad 11 **NO:** Actividad 9.	Director de Gobernanza de TI e Innovación	Plan de Seguridad Informática revisado.
11	Revisar el Plan de Seguridad Informática	Revisa el Plan de Seguridad Informática, actualizado. ¿Se aprueba? **SI:** Actividad 12 **NO:** Actividad 9	Coordinador General de Tecnologías de Información y Comunicación	Plan de Seguridad Informática propuesto
12	Aprobar suscribir el Plan de Seguridad Informática	El Comité de Tecnologías de Información y Comunicación, aprueba el Plan de Seguridad Informática, ¿Se aprueba? **SI:** FIN **NO:** Actividad 11	Comité de Tecnologías de Información y Comunicación	Plan de Seguridad Informática aprobado

4. DESCRIPCIÓN DEL SUBPROCESO DE IMPLEMENTACIÓN DEL PLAN DE SEGURIDAD INFORMÁTICA

4.1. FICHA DEL SUBPROCESO DE IMPLEMENTACIÓN DEL PLAN DE SEGURIDAD INFORMÁTICA

Descripción:	**DISPARADOR:** *Necesidad de implementar los controles definidos en Plan de Implementación de Controles de Seguridad Informática.* **ENTRADAS:** ❖ *Plan de Implementación de Controles de Seguridad Informática.* ❖ *Informes de monitoreo por aplicación de controles de seguridad informática.*
Productos/Servicios del proceso:	❖ *Políticas, estándares y marcos de referencia para el gobierno de TI.* ❖ *Informes de la ejecución del Aseguramiento de Calidad y Seguridad Informática.*

4.2. NORMAS ESPECÍFICAS DEL SUBPROCESO DE IMPLEMENTACIÓN DEL PLAN DE SEGURIDAD INFORMÁTICA.

- La aprobación y actualizaciones del Plan de Implementación de Controles de Seguridad Informática, sustenta el inicio de la Implementación del Plan de Seguridad Informática, el cual contiene los controles técnicos priorizados a ser implementados en los activos informáticos en base al análisis de riesgos tecnológicos.

- El Equipo de Gestión de Seguridad Informática será conformado por un Líder de Equipo de la Dirección de Gobernanza de TI e Innovación y al menos un técnico de cada unidad de la Coordinación General de Tecnologías de Información y Comunicación con conocimientos afines al control a ser implementado.

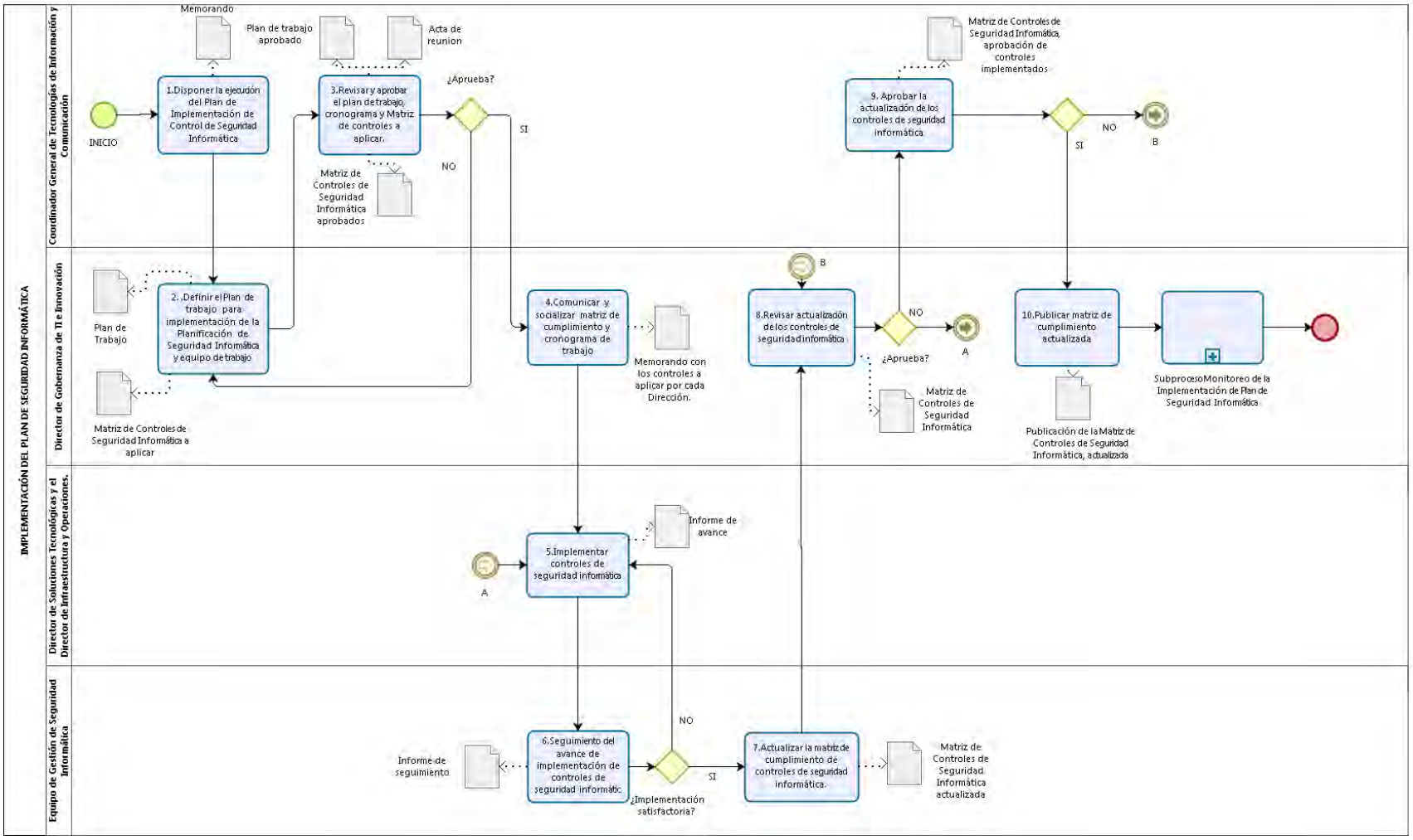
- La formalización de los equipos de trabajo se efectuará mediante acta suscrita por el Coordinador de General de Tecnologías de Información y Comunicación, el Director de Gobernanza de TI e Innovación y el Director de Soluciones Tecnológicas y/o el Director de Infraestructura y Operaciones, según la proveniencia de los recursos involucrados.

- El seguimiento y aplicación de controles de seguridad informática se controlará mediante el Plan de Trabajo para Implementación de la Planificación de Seguridad Informática que incluye el cronograma de trabajo.

- La implementación de controles de seguridad informática se registrará en la Matriz de Controles de Seguridad Informática, la cual será alimentada por el Equipo de Gestión de Seguridad Informática bajo la supervisión del Director de Gobernanza de TI e Innovación, incluirá información referencial a su operación, así como la definición de indicadores de alerta.

- La Matriz de Controles de Seguridad Informática, será comunicada formalmente al responsable del Plan Director de Seguridad de Información, cada vez que se implemente un control programado, esta matriz será publicada en el servidor documental Alfresco con la autorización del Director de Gobernanza de TI e Innovación.

4.3. DIGRAMA DE FLUJO DEL SUBPROCESO DE IMPLEMENTACIÓN DEL PLAN DE SEGURIDAD INFORMÁTICA.



4.4. DESCRIPCIÓN DE ACTIVIDADES DEL SUBPROCESO DE IMPLEMENTACIÓN DEL PLAN DE SEGURIDAD INFORMÁTICA

#	Actividad	Descripción	Responsable	Documentos generados
1	Disponer la ejecución del Plan de Implementación de Control de Seguridad Informática	Se emitirá los lineamientos para ejecución del Plan de Implementación de Control de Seguridad Informática, dirigido al Director de Gobernanza de TI e Innovación.	Coordinador General de Tecnologías de Información y Comunicación	Memorando
2	Definir el Plan de trabajo para implementación de la Planificación de Seguridad Informática y equipo de trabajo.	Se revisará de manera detallada los controles, prioridades establecidas en el **Subproceso Planificación de Controles de Seguridad informática** para determinar el plan de trabajo tomando en cuenta cronogramas de implementación, recursos tecnológicas, no tecnológicos y definir el equipo de trabajo, con la participación del Director de Gobernanza de TI e Innovación, Director de Soluciones Tecnológicas y el Director de Infraestructura y Operaciones.	Director de Gobernanza de TI e Innovación	Plan de Trabajo y Matriz de Controles de Seguridad Informática a aplicar
3	Revisar y aprobar el plan de trabajo, cronograma y Matriz de controles a aplicar.	Se presentará el Plan de Trabajo y Matriz de Controles a aplicar para aprobación del Coordinador General de Tecnologías de Información y Comunicación, con la participación del Director de Gobernanza de TI e Innovación, Director de Soluciones Tecnológicas y el Director de Infraestructura y Operaciones. ¿Aprueba? **SI:** Actividad 4 **NO:** Actividad 2.	Coordinador General de Tecnologías de Información y Comunicación	Acta / Plan de Trabajo y Matriz de Controles de Seguridad Informática aprobados
4	Comunicar y socializar matriz de cumplimiento y cronograma de	Se efectuará la comunicación formal de la matriz de cumplimiento y cronograma de trabajo al Equipo de Trabajo con la participación	Director de Gobernanza de TI e Innovación	Acta de reunión y memorando con los controles a aplicar por cada Dirección.

#	Actividad	Descripción	Responsable	Documentos generados
	trabajo	del Director de Gobernanza de TI e Innovación, Director de Soluciones Tecnológicas y el Director de Infraestructura y Operaciones.		
5	Implementar controles de seguridad informática	Se implementará los controles de seguridad informática bajo el plan de trabajo aprobado según la disponibilidad de recursos, esta actividad estará a cargo del Director de Soluciones Tecnológicas y el Director de Infraestructura y Operaciones.	Director de Soluciones Tecnológicas y el Director de Infraestructura y Operaciones	Informes de avance
6	Seguimiento del avance de implementación de controles de seguridad informática	Se efectuará el seguimiento del avance de la implementación de controles de seguridad informática. ¿Implementación satisfactoria? **SI:** Actividad 7 **NO:** Actividad 5	Equipo de Gestión de Seguridad Informática	Informe de seguimiento
7	Actualizar la matriz de cumplimiento de controles de seguridad informática	Se procederá con la actualización de la matriz de cumplimiento de controles respecto de la implementación efectuada para cada control.	Equipo de Gestión de Seguridad Informática	Matriz de Controles de Seguridad Informática actualizada
8	Revisar actualización de los controles de seguridad informática	Se revisará la implementación de cada control de seguridad informática para aprobación del Coordinador General de Tecnologías de Información y Comunicación ¿Aprueba? **SI:** Actividad 9 **NO:** Actividad 5.	Director de Gobernanza de TI e Innovación	Matriz de Controles de Seguridad Informática
9	Aprobar la actualización de los controles de seguridad informática	El Coordinador General de Tecnologías de Información y Comunicación revisa la Matriz de Controles de Seguridad Informática para publicar el cumplimiento de actualización. ¿Aprueba? **SI:** Actividad 10 **NO:** Actividad 8	Coordinador General de Tecnologías de Información y Comunicación	Matriz de Controles de Seguridad Informática, aprobación de controles implementados
10	Publicar matriz de cumplimiento	Se procederá con la publicación de la Matriz de	Director de Gobernanza de	Publicación de la Matriz de

#	Actividad	Descripción	Responsable	Documentos generados
	actualizada	Controles de Seguridad Informática actualizada, en el Servidor Documental Alfresco para uso interno	TI e Innovación	Controles de Seguridad Informática, actualizada
Subproceso		**Monitoreo de la Implementación de Plan de Seguridad Informática**	**Director de Gobernanza de TI e Innovación**	

5. DESCRIPCIÓN DEL SUBPROCESO DE MONITOREO DE LA IMPLEMENTACIÓN DEL PLAN DE SEGURIDAD INFORMÁTICA

5.1. FICHA DEL SUBPROCESO

Descripción:	**DISPARADOR:** ❖ *Necesidad de establecer la vigencia y efectividad de la implementación de los controles de seguridad informática.* ❖ *La ejecución de este subproceso es permanente para cada control implementado por recurso tecnológico, finalizará únicamente cuando el recurso sea cambiado o eliminado del inventario tecnológico.* **ENTRADAS:** ❖ *Plan de Implementación de Controles de Seguridad Informática.*
Productos/Servicios del proceso:	❖ *Informes de la ejecución del aseguramiento de calidad y seguridad informática.*

5.2. NORMAS ESPECÍFICAS DEL SUBPROCESO DE MONITOREO DE LA IMPLEMENTACIÓN DEL PLAN DE SEGURIDAD INFORMÁTICA

- Una vez implementados los controles informáticos, serán incluidos en el proceso de monitoreo periódico y continuo para establecer su vigencia y operación adecuada.

- El Equipo de Monitoreo de Implementación de Controles de Seguridad Informática será conformado por un Líder de Equipo de la Dirección de Gobernanza de TI e Innovación y al menos un técnico de cada unidad de la Coordinación General de Tecnologías de Información y Comunicación con conocimientos afines al control a ser implementado.

- La formalización de los equipos de trabajo se efectuará mediante acta suscrita por el Coordinador de General de Tecnologías de Información y Comunicación, el Director de Gobernanza de TI e Innovación y el Director de Soluciones Tecnológicas y/o el Director de Infraestructura y Operaciones, según la proveniencia de los recursos involucrados.

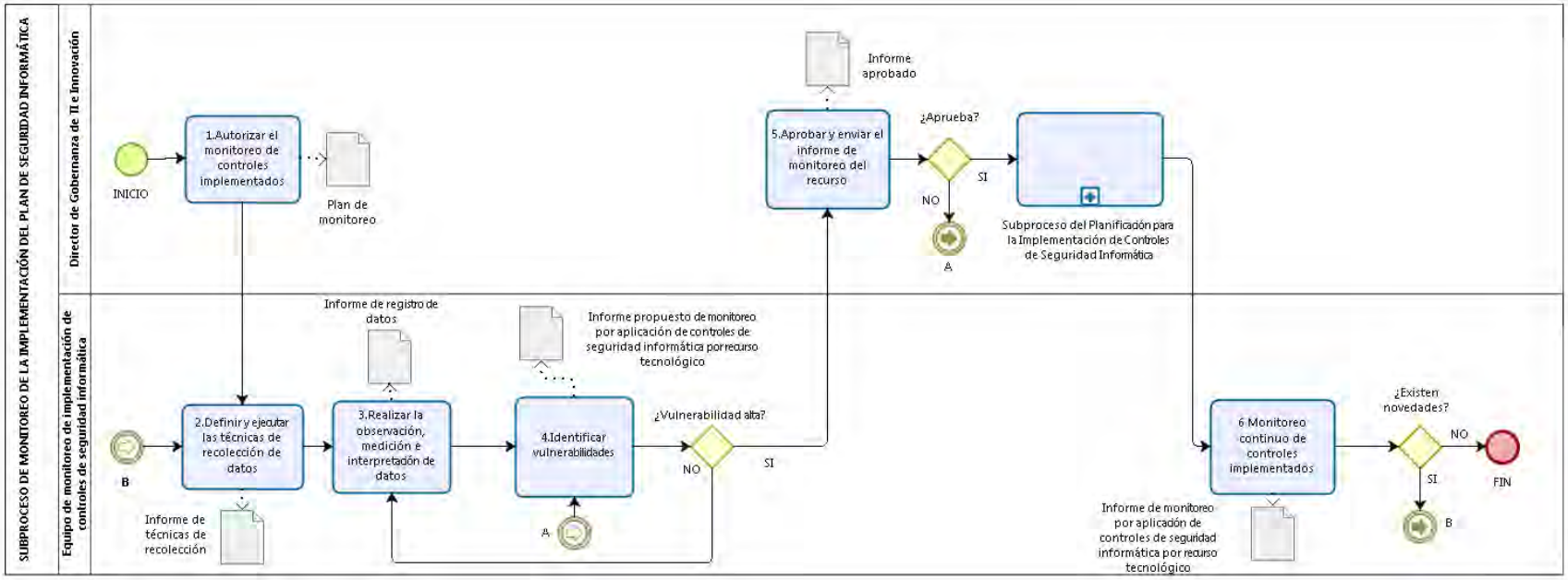
- El Equipo de Trabajo definirá las técnicas de recolección de datos más aplicables para monitorear cada control implementado, así como la periodicidad de su obtención.

- La detección de vulnerabilidades de operación de los controles de seguridad informática implementados deberá ser puesta en conocimiento del Director de Gobernanza de TI e Innovación.

- La operación anómala verificada de cualquier control implementado, deberá ser notificada por el Director de Gobernanza de TI e Innovación al proceso de Planificación de Controles de Seguridad Informática para que se inicie su revisión técnica.

- Los informes generados por el proceso de Monitoreo de Implementación de Controles de Seguridad Informática, serán publicados en el servidor documental Alfresco con la autorización del Director de Gobernanza de TI e Innovación.

5.3. DIAGRAMA DE FLUJO DEL SUBPROCESO DE MONITOREO DE LA IMPLEMENTACIÓN DEL PLAN DE SEGURIDAD INFORMÁTICA



5.4. DESCRIPCIÓN DE ACTIVIDADES DEL SUBPROCESO DE MONITOREO DE LA IMPLEMENTACIÓN DEL PLAN DE SEGURIDAD INFORMÁTICA.

#	Actividad	Descripción	Responsable	Documentos generados
1	Autorizar el monitoreo de controles implementados.	Se establecerán responsabilidades, periodicidad, herramientas, indicadores, estadísticas, métricas de monitoreo.	Director de Gobernanza de TI e Innovación	Plan de monitoreo
2	Definir y ejecutar las técnicas de recolección de datos	Se definirán las técnicas de recolección de datos para construir o seleccionar los instrumentos que permitan obtener datos del recurso monitoreado.	Equipo de monitoreo de implementación de controles de seguridad informática	Informe de técnicas de recolección
3	Realizar la observación, medición e interpretación de datos	Se efectuará la observación, medición e interpretación de los datos observados. Mediante indicadores, métricas.	Equipo de monitoreo de implementación de controles de seguridad informática	Informe de registro de datos
4	Identificar vulnerabilidades	Se identificarán vulnerabilidades o deficiencias de la operación de los controles de seguridad implementados, estableciendo el nivel de afectación en la operación del recurso tecnológico, incluye recomendaciones. ¿Vulnerabilidad alta? **SI**: Actividad 5 **NO**: Actividad 3	Equipo de monitoreo de implementación de controles de seguridad informática	Informe propuesto de monitoreo por aplicación de controles de seguridad informática por recurso tecnológico
5	Aprobar y enviar el informe de monitoreo del recurso	Se aprobará y enviará el informe de monitoreo del recurso para la aplicación de acciones correctivas en el **Subproceso del Planificación de Controles de Seguridad Informática.** ¿Aprueba? **SI:** Subproceso del Planificación de Controles de Seguridad Informática **NO:** Actividad 4	Director de Gobernanza de TI e Innovación	Informe aprobado de monitoreo por aplicación de controles de seguridad informática por recurso tecnológico
Subproceso		**Planificación de Controles de Seguridad Informática**		
6	Monitorear continuamente	Se efectuará el monitoreo periódico de los controles	Equipo de Gestión de	Informes de la ejecución del

#	Actividad	Descripción	Responsable	Documentos generados
	de controles implementados.	implementados, incluye métricas vulnerabilidades. ¿Existen novedades? SI: Actividad 2 NO: (FIN)	Seguridad Informática	aseguramiento de calidad y seguridad informática aprobado.

6. INDICADORES DE GESTIÓN DEL PROCESO GESTION DE LA SEGURIDAD INFORMATICA.

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

7. TÉRMINOS Y DEFINICIONES

Controles de Seguridad Informática: Establece las acciones técnicas implementadas en la infraestructura tecnológica y sistemas de información orientadas a mantener niveles aceptados de confidencialidad, integridad y disponibilidad aceptados por la organización.

Ethical hacking: Comprende la ejecución de pruebas de penetración, pruebas de intrusión o equipo rojo, con la finalidad de localizar debilidades y vulnerabilidades de los servicios informáticos y la infraestructura tecnológica sobre la cual operan mediante la duplicación de la intención y las acciones de ataques informáticos.

ISO: Organización Internacional de Estandarización.

PAC: Plan Anual de Contratación.

PEI: Plan Estratégico Institucional.

PETI: Plan Estratégico Tecnológico.

8. LISTADO DE DOCUMENTOS YANEXOS.

8.1. DOCUMENTOS.

Código	Nombre del documento	Ubicación Física	Ubicación Digital
F-GSI-1	Plan de Implementación de Controles de Seguridad Informática		Servidor documental: Documentos> C.G.T> GCS> Seguridad Informática
F-GSI-2	Plan de Riesgos		Servidor documental: Documentos> C.G.T> GCS> Seguridad

	Tecnológicos		Informática
F-GSI -3	Matriz de Controles de Seguridad Informática		Servidor documental: Documentos> C.G.T> GCS> Seguridad Informática
F-GSI -4	Plan de trabajo		Servidor documental: Documentos> C.G.T> GCS> Seguridad Informática
F-GSI -5	Plan de monitoreo		Servidor documental: Documentos> C.G.T> GCS> Seguridad Informática
F-GSI -6	Informes técnicos		Servidor documental: Documentos> C.G.T> GCS> Seguridad Informática

8.2. ANEXOS

N/A