Suprema Corte
de Justicia de la Nación

Manual del Sistema de Gestión de Seguridad de la Información

Dirección General de Tecnologías de la Información

Dirección de Seguridad Informática

Oficialía Mayor

Contenido

1 Introducción

La Suprema Corte de Justicia de la Nación (SCJN), a través de los responsables de procesos de seguridad informática, establece a la seguridad informática como un aspecto vital para asegurar la consecución de los objetivos institucionales y para mantener el cumplimiento normativo y regulatorio.

La Dirección de Seguridad Informática (DSI) ha tomado la decisión de establecer, implementar, mantener y mejorar un Sistema de Gestión de Seguridad de la Información (SGSI) que ayude a proteger la confidencialidad, integridad y disponibilidad de la información, como parte de una estrategia orientada a la administración del riesgo y a la consolidación de la seguridad informática en la DSI y en la Dirección General de Tecnologías de la Información (DGTI).

Un SGSI es un conjunto de elementos interrelacionados (estructura organizacional, políticas, planificación de actividades, responsabilidades, procesos, procedimientos y recursos) que utiliza una organización para establecer una política y unos objetivos de seguridad informática, tomando como base el enfoque de gestión del riesgo y mejora continua.

2 Objetivo

Definir el marco gestor y aspectos particulares de la seguridad informática en la SCJN, con base en estándares internacionales y mejores prácticas, congruentes con la política de seguridad informática, la misión y visión de la SCJN, con el fin de promover, mantener y mejorar las medidas de seguridad informática institucionales.

3 Conceptos Generales

Término	Definición
Acción correctiva	Es la acción que se realiza para eliminar la causa de una no conformidad detectada.
Acción Preventiva	Es la medida que ayuda a prevenir la materialización de una no conformidad.
Activo de información	Es la información o datos que son de valor para la organización como registros de usuarios, propiedad intelectual o información en general.
Amenaza	Es el posible acto o circunstancia interna o externa que puede explotar, de manera intencional o circunstancial, la debilidad presente en un activo de información.
Análisis de riesgos	Es el uso sistemático de la información para identificar las fuentes de vulnerabilidades y amenazas de los activos críticos, infraestructura tecnológica o activos de información, así como efectuar la evaluación de su magnitud o impacto y estimar los recursos necesarios para su prevención o mitigación.
Auditoría	Proceso sistemático, independiente y documentado para obtener evidencia de auditoría y evaluarla objetivamente para determinar en qué medida se cumplen los criterios de auditoría.
Confidencialidad	Característica o propiedad por la cual la información sólo es revelada a individuos o procesos autorizados.

Control de seguridad	Es una medida utilizada para prevenir, detectar, mitigar o recuperarse ante la materialización de una amenaza, y tiene por función permitir, vigilar, conocer su estado de operación y mantener dentro de los parámetros aceptables un riesgo de seguridad.
DGTI	Dirección General de Tecnologías de la Información.
Disponibilidad	Propiedad que asegura que los activos de la información son utilizables para personal autorizado en su uso y demanda.
DSI	Dirección de Seguridad Informática.
Impacto	Son las consecuencias últimas en la organización como resultado de la materialización de una amenaza.
Información	Conjunto de datos organizados en poder de una entidad que posean valor para la misma, independientemente de la forma en que se guarde o transmita de su origen o de la fecha de elaboración.
Integridad	Propiedad que asegura que la información no es alterada sin autorización en su transporte, procesamiento o almacenamiento.
Mejora continua	Actividad recurrente para mejorar el rendimiento del SGSI.
Partes interesadas	Persona u organización que puede afectar, verse afectada, o percibirse como afectada por una decisión o actividad.
Riesgo	Probabilidad de que una amenaza pueda explotar una vulnerabilidad, generando un impacto sobre la infraestructura tecnológica y los activos críticos de la Corte.
SCJN	Suprema Corte de Justicia de la Nación
Sistema Informático	El conjunto de componentes o programas construidos con herramientas de software que habilitan una funcionalidad o automatizan un proceso, de acuerdo con requerimientos previamente definidos.

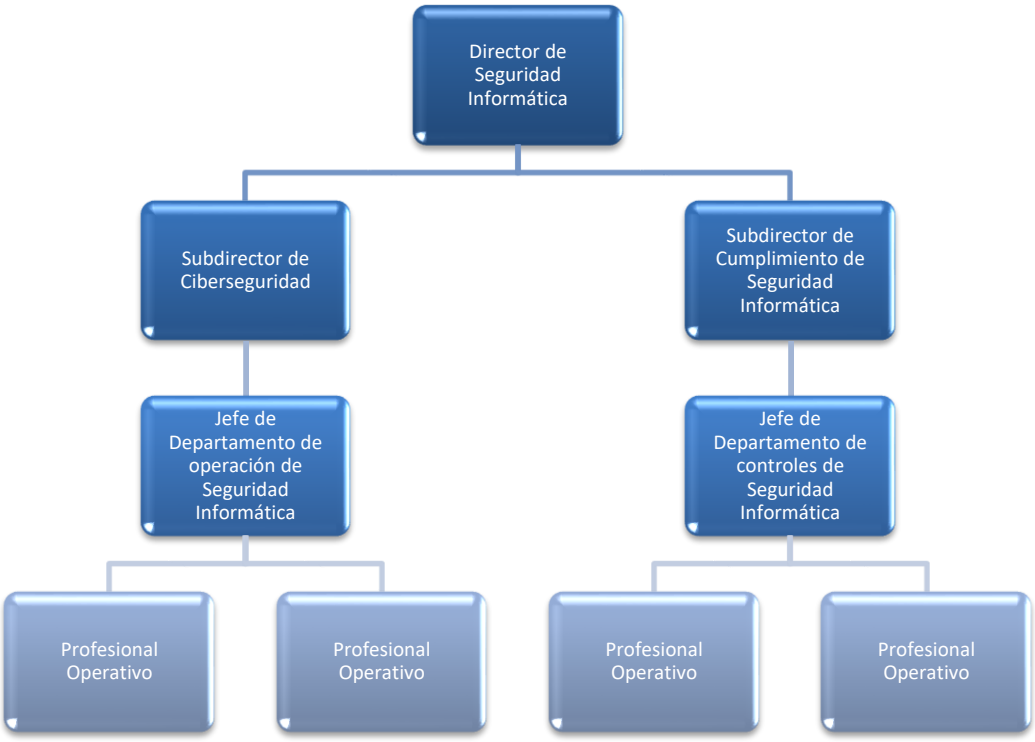
4 Contexto de la Organización

4.1 Comprender la organización y su contexto

La DSI es un área que forma parte de la DGTI, cuyo objetivo es coordinar, planear y proponer los procedimientos, estrategias, soluciones, controles y herramientas de seguridad informática y de ciberseguridad que permitan garantizar la integridad, la disponibilidad y la confiabilidad de los sistemas informáticos de la SCJN.

La DSI se conforma por una Subdirección de Ciberseguridad, un Departamento de Operación de Seguridad Informática, una Subdirección de Cumplimiento de Seguridad Informática y un Departamento de Controles de Seguridad Informática, como se muestra a continuación en su organigrama:

- **Organigrama**



A su vez, a continuación, se describen las funciones y objetivos principales de las áreas que conforman a la DSI:

Subdirección de Ciberseguridad: Tiene el objetivo de proponer, implementar, monitorear y analizar los mecanismos de seguridad informática y de ciberseguridad para la protección de los sistemas informáticos de la SCJN.

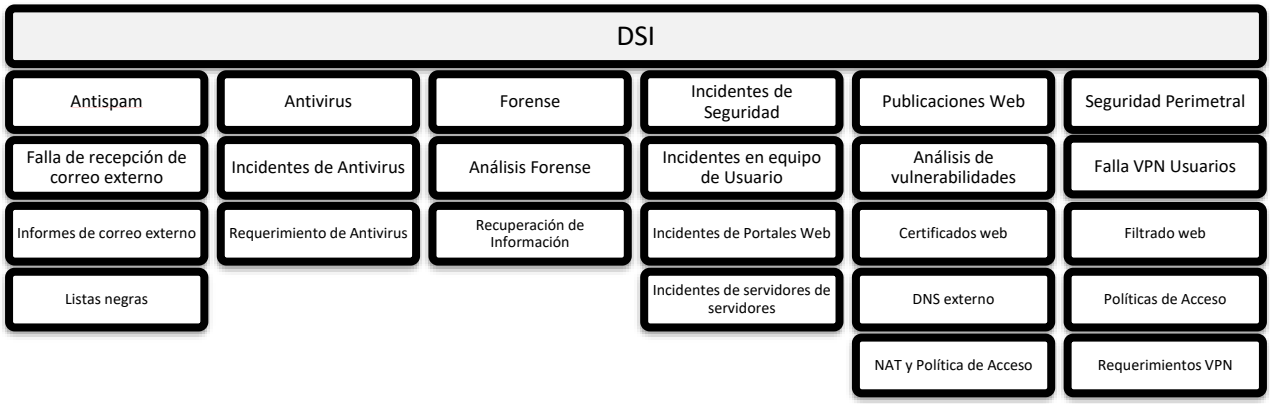
Subdirección de Cumplimiento de Seguridad Informática: Gestiona y supervisa el Sistema de Gestión de Seguridad de la Información, coordinando las acciones de implementación de los controles mínimos que permitan dar cumplimiento tanto con las mejores prácticas en términos de seguridad informática como con la normatividad aplicable vigente.

Departamento de Operación de Seguridad Informática: Operar las soluciones de seguridad informática y de ciberseguridad, con base en las mejores prácticas, con la finalidad de fortalecer la protección de la confidencialidad, integridad y disponibilidad de los sistemas informáticos de la SCJN.

Departamento de Controles de Seguridad Informática: Dar seguimiento a la implementación de los controles del SGSI, tramitar la documentación y evidencia que permita evaluar y mejorar dicho Sistema de Gestión, así como contar con los indicadores e información oportuna para toma de decisiones en cuestiones de seguridad informática al interior de la SCJN.

- **Procesos operativos de la DSI**

Actualmente, la DSI cuenta con seis servicios principales y veinte subservicios que se proporcionan a las diferentes áreas de la DGTI. A continuación, se muestra el catálogo:



- **Descripción de servicios principales**

Los principales servicios mostrados en el esquema anterior refieren a la siguiente descripción:

Antispam: El servicio de antispam tiene el objetivo de restringir los correos electrónicos no deseados de manera automática, con la finalidad de prevenir posibles ataques de ingeniería social como el phishing, dentro de la corte.

Antivirus: La DSI proporciona el servicio de antivirus, el cual es una solución que ayuda a detectar y mitigar software malicioso antes de que éste afecte a equipos y dispositivos de la SCJN.

Forense: Es el servicio que busca la obtención, preservación y documentación de evidencia digital en equipos o dispositivos de cómputo de usuarios o de servidores de datos, para determinar las causas que han originado un incidente de seguridad informática o una vulnerabilidad a la confidencialidad, integridad o disponibilidad de la información de alguna de las áreas de la SCJN.

Incidentes de Seguridad: El servicio de Incidentes de Seguridad busca identificar, atender y dar seguimiento a los incidentes de seguridad informática para contener el impacto que estos puedan ocasionar en la infraestructura tecnológica de la SCJN.

Publicaciones Web: Servicio de Seguridad Informática que consta de la configuración de herramientas tecnológicas, asignación de certificados y análisis de vulnerabilidades para la publicación de un portal web de la SCJN en internet.

Seguridad Perimetral: Gestionar las políticas de los dispositivos de seguridad perimetral, así como gestionar los accesos a los servicios de las redes internas LAN/WAN, por parte de los usuarios de la SCJN, para establecer una mayor protección contra flujos de red y protocoles inseguros.

Dichos servicios, son gestionados a través de los siguientes procedimientos operativos:

- Procedimiento para el Análisis de Vulnerabilidades de la Infraestructura Tecnológica de Aplicaciones de la SCJN.
- Procedimiento para el Análisis Forense Informático.
- Procedimiento para la Administración de Borrado Seguro en Dispositivos Informáticos.
- Procedimiento para la Administración de Políticas de Seguridad Perimetral y de Filtrado de Contenido.
- Procedimiento de Respuesta a Incidentes de Seguridad Informática.
- Procedimiento para la recuperación de información.

- **FODA**

Como parte de este apartado del SGSI, a continuación, se presenta el análisis de fortalezas, oportunidades, debilidades y amenazas en términos de seguridad informática:

✓ **Fortalezas**
- Directrices sobre la seguridad en los servicios informáticos consideradas en las Líneas Generales de Trabajo 2023 – 2026 de la Ministra Presidente de la SJCN.
- Se cuenta con un proveedor de servicios que ayuda a fortalecer varios aspectos de seguridad de la información, como el monitoreo de amenazas avanzadas, ciber inteligencia, análisis de vulnerabilidades y establecimiento de marcos de trabajo.
- Se cuenta con el interés y apoyo de la Dirección General para la implementación, mantenimiento y mejora del SGSI.

✓ **Oportunidades**
- Hay una demanda creciente en servicios de seguridad Informática y ciberseguridad. Tenía que abordar.
- Los funcionarios de la SCJN tienen posibilidad de capacitarse y ampliar su conocimiento en temas de seguridad informática.
- Los funcionarios de la DGTI pueden integrar el enfoque de riesgos en su operación habitual.

✓ **Debilidades**
- Dependencia de la DSI en áreas internas de la DGTI para recopilar y consolidar información necesaria para la gestión de riesgos.
- Al hacer la concientización de todo el personal de la SCJN en temas, conceptos y responsabilidades de seguridad informática.

✓ **Amenazas**
- Actualmente México es el primer país en Latinoamérica que sufre ataques cibernéticos.
- La rotación de funcionarios especializados de las áreas de la DGTI podría poner en riesgo la continuidad del SGSI.

4.2 Entendimiento de las necesidades y expectativas de las partes interesadas

La DSI ha determinado las partes que son relevantes para su SGSI, tomando en cuenta el cumplimiento de las Líneas Generales de Trabajo de la Ministra Presidente de la SCJN, los servicios que ofrece como DSI y las herramientas o capacidades que necesitan sus funcionarios para poder operar con eficacia dentro de un SGSI.

Las principales partes interesadas se muestran a continuación:

Partes interesadas de la DSI	Necesidades / Expectativas
Dirección General de Tecnologías de la Información	La Dirección General busca que exista un cumplimiento a la Líneas Generales de Trabajo, además de verificar la eficacia de la DSI como proveedor interno de servicios respecto a sus servicios principales y al cumplimiento de los controles de seguridad informática del SGSI.
Áreas internas de la DGTI	La DSI debe asegurarse de que proporciona un servicio adecuado a las áreas internas de la DGTI y que cumple con sus requerimientos (sobre todo en los servicios principales).
Funcionarios de la DSI	Los funcionarios de la DSI deben velar por la seguridad de los activos críticos de la institución, por lo que se debe brindar capacitación orientada a cubrir las actividades enfocadas a salvaguardar la confidencialidad, integridad y disponibilidad de estos.

4.3 Alcance del Sistema de Gestión de Seguridad de la Información

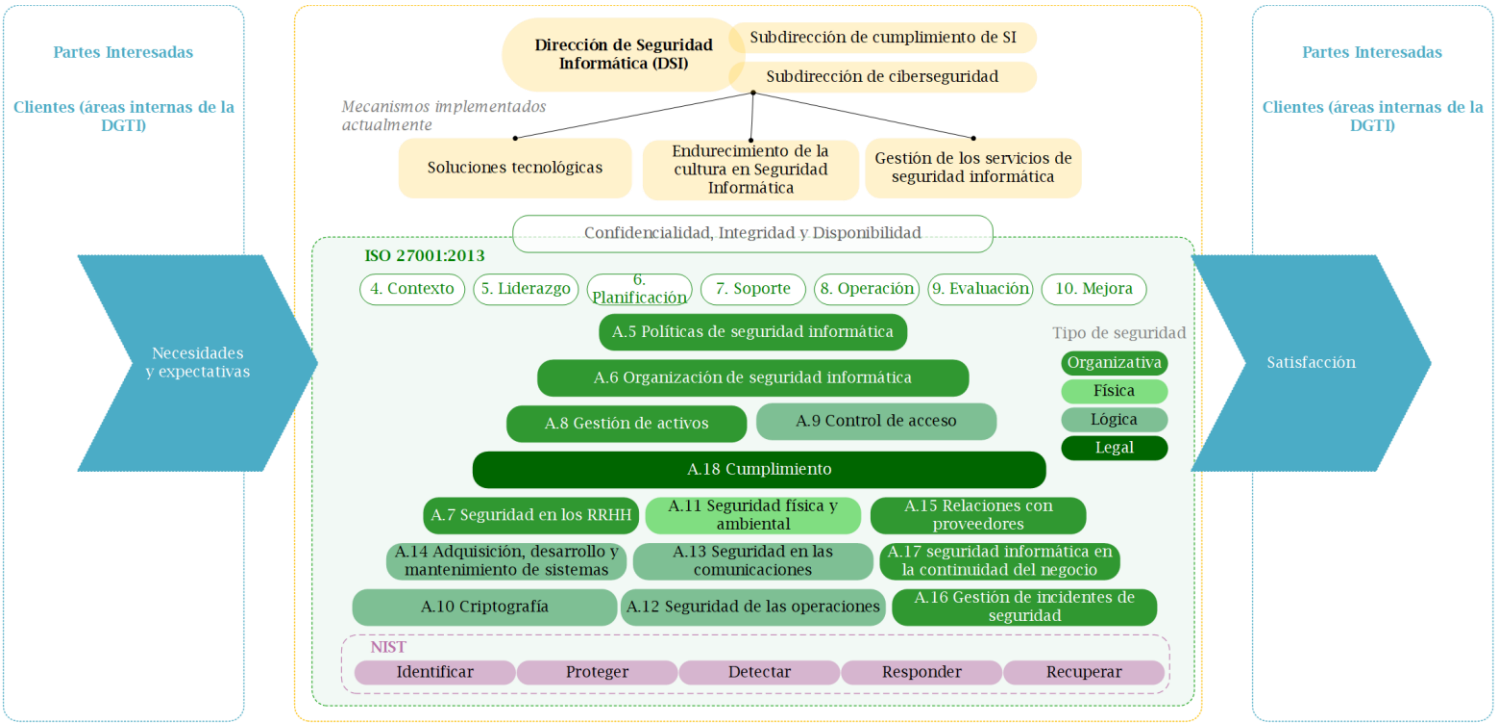
La DSI, en función de los resultados de diferentes análisis para determinar la criticidad de los diferentes procesos y la viabilidad de un proyecto enfocado a la certificación ISO/IEC 27001, ha establecido el alcance del SGSI a los servicios de **Análisis de Vulnerabilidades de la Infraestructura Tecnológica de Aplicaciones de la SCJN** y de **Respuesta a Incidentes de Seguridad Informática,** los cuales son fundamentales para mantener la confidencialidad, integridad, disponibilidad y el no repudio de la información durante las operaciones de las diferentes áreas de la DGTI, así como el logro de los objetivos institucionales.

4.4 Sistema de Gestión de Seguridad de la Información

La DSI establece, implementa, mantiene y mejora continuamente un SGSI, de acuerdo con los requisitos del estándar internacional ISO/IEC 27001:2013.

A continuación, se presenta el esquema del SGSI:

- **Mapa del SGSI de la DSI**



El SGSI se opera sobre los tres ejes esenciales de la DSI, que son: soluciones tecnológicas, endurecimiento de la cultura en seguridad informática y gestión de los servicios de seguridad informática.

Sobre estos tres ejes, se identificaron los controles de seguridad informática que son aplicables y que ayudan a robustecer la confidencialidad, integridad y disponibilidad de la información, dividiendo controles de acuerdo con el tipo de seguridad (organizativa, física, lógica y legal).

Por lo anteriormente mencionado, la DSI ejecuta las actividades necesarias para dar cumplimiento con las cláusulas y requerimientos del estándar, implementando y dando mantenimiento a procesos operativos y de soporte.

5 Liderazgo

5.1 Compromiso y liderazgo

La alta dirección demuestra el liderazgo y compromiso con respecto al Sistema de Gestión de Seguridad de la Información a través de:

- El estableciendo una política de seguridad de seguridad informática (ver apartado 5.2) y objetivos del SGSI que son compatibles con las Líneas Generales de Trabajo de la Ministra Presidente (acatando el lineamiento de operar bajo un enfoque en riesgos).

- La integración de los requisitos del SGSI en las actividades de la DSI, en sus procesos y de manera general en todos los mecanismos que se requieren para la operación, mantenimiento, revisión y mejora del SGSI.

- La provisión de los recursos necesarios, a través de la asignación y nombramiento de roles necesarios para la operación del SGSI.

- El fortalecimiento de la conciencia de seguridad informática en los funcionarios de la involucrados, promoviendo el uso de una plataforma disponible en línea para la adquisición de conocimientos en seguridad informática y ciberseguridad.

5.2 Política

"La Dirección de Seguridad Informática (DSI) de la Suprema Corte de Justicia de la Nación (SCJN) reconoce y entiende la importancia de la gestión de sus activos informáticos para asegurar la confidencialidad, integridad y disponibilidad de la información creada, procesada, transmitida o resguardada en ellos, con el fin de establecer un marco de confianza en sus deberes y en la operación de la infraestructura tecnológica que soporta los servicios otorgados a la ciudadanía, en estricto cumplimiento de obligaciones legales y en concordancia con la misión y visión de la SCJN.

La DSI establecerá mecanismos para la gestión sistemática de riesgos y aplicación de controles a fin de proteger los activos informáticos de amenazas internas o externas mediante la implementación, revisión y mejora de un Sistema de Gestión de Seguridad de la Información basado en el estándar ISO/IEC 27001 que permita fortalecer la gestión de servicios que brinda a las áreas de la Dirección General de Tecnologías de la Información, principalmente los de análisis de vulnerabilidades de la infraestructura tecnológica de aplicaciones de la SCJN y el servicio de respuesta a incidentes de seguridad informática."

De acuerdo con las necesidades correspondientes de seguridad informática, la DSI ha definido objetivos principales para el SGSI (ver apartado 6.2), los cuales nacen como puntos esenciales que ayudan cumplir con la Política de Seguridad de la Organización.

La DSI tiene el compromiso de revisar y adecuar la presente política de seguridad de la información, de acuerdo con las necesidades de este alto tribunal, así como parte de la mejora continua del SGSI.

5.3 Roles y responsabilidades

Los actores del SGSI están descritos en los roles y equipos de trabajo correspondientes, a continuación, se hace una síntesis de sus responsabilidades:

Alta dirección	
RACI	**Participantes**
Aprobador y Responsable	Director de Seguridad Informática
Funciones sustantivas	
• Definir la estrategia de la seguridad informática en la SCJN e implementación del SGSI.	

• Asignar recursos y responsabilidades, así como verificar y aprobar las directrices de seguridad informática. • Aprobar y asegurar la difusión de la política de seguridad informática institucional. • Supervisar el plan de gestión riesgos y las posibles soluciones para mitigar amenazas.
Grupo Modelo de Gobierno de Seguridad Informática
Grupo Estratégico de Seguridad Informática (GESI)

Responsable del Sistema de Gestión de Seguridad de la Información	
RACI	**Participantes**
Aprobador	Director de Seguridad Informática
Responsables	• Subdirector de Cumplimiento de Seguridad Informática • Jefa de Departamento de Controles de Seguridad informática
Consultados / Informados	• Subdirector de Ciberseguridad • Jefe de Departamento de Operaciones de Seguridad informática • *Subdirector General de Planeación y Control de Proyectos Tecnológicos (SGPCPT)*
Funciones sustantivas	
• Liderar la implantación del SGSI. • Dar seguimiento a la correcta ejecución de los procesos de seguridad informática. • Elaborar, promover y mantener la política de seguridad informática institucional. • Proponer nuevos objetivos en materia de seguridad informática. • Supervisar y mantener cumplimiento del marco normativo de seguridad informática. • Validar la implantación de los requisitos de seguridad identificados y establecidos.	
Grupo Modelo de Gobierno de Seguridad Informática	
Grupo Responsable de Seguridad Informática (GRSI)	

Equipo Auditor	
RACI	**Participantes**
Aprobador	Director de Seguridad Informática
Responsables	• Subdirector de Cumplimiento de Seguridad Informática • Jefa de Departamento de Controles de Seguridad informática • Los funcionarios que se consideren para conservar la imparcialidad
Consultado	*Subdirector General de Planeación y Control de Proyectos Tecnológicos (SGPCPT)*
Funciones sustantivas	
• Establecer los criterios y métodos a través de los cuales se realizarán las actividades de auditoría interna. • Realizar auditoría(s). • Identificar desviaciones y hacer recomendaciones de mejora para garantizar la efectividad del proceso. • Presentar resultados de Auditoría. • Dar seguimiento a la resolución de hallazgos de Auditoría.	
Grupo Modelo de Gobierno de Seguridad Informática	

Grupo Responsable de Seguridad Informática (GRSI)

Responsable de Ciberseguridad	
RACI	**Participantes**
Aprobador	Director de Seguridad Informática
Responsables	• Subdirector de Ciberseguridad • Jefe de Departamento de Operaciones de Seguridad informática
Consultados / Informados	• Proveedores de servicios • Fabricantes de soluciones tecnológicas • Partes interesadas
Funciones sustantivas	
• Otorgar la información necesaria para mantener actualizado el catálogo de activos. • Diseño, implementación y mantenimiento de mecanismos propios para la protección de la infraestructura involucrada en el alcance, así como contribuir en la ejecución del análisis de riesgos y su tratamiento.	
Grupo Modelo de Gobierno de Seguridad Informática	
Equipo de Implementación y Supervisión de Controles de seguridad Informática (EISC)	

Equipo de Gestión de Riesgos			
RACI	**Participantes**	**Rol SGSI-Riesgos**	**Funciones sustantivas**
Aprobador	Director de Seguridad Informática	Aprobador	Supervisar el plan de gestión riesgos y las posibles soluciones para mitigar amenazas.
Responsables	Subdirector de Cumplimiento de Seguridad Informática	Responsable de Gestión de Riesgos	Seguimiento y revisión de las actividades propias de la ejecución del análisis de riesgos.
	Jefa de Departamento de Controles de Seguridad informática	Gestor de riesgos	Ejecutar de las actividades para realizar la gestión de riesgos (evaluación, propuesta, diseño y seguimiento a la implementación de mecanismos para el control de los riesgos).
Responsables y Consultados / Informados	Subdirector de Ciberseguridad	Implementador de acciones de control	Analizar, aprobar, ejecutar y validar los mecanismos de control a los riesgos identificados en función a las capacidades y recursos, así como justificar la no viabilidad de la implementación.
	Jefe de Departamento de Operaciones de Seguridad informática		
	Administradores de sistemas		
	Proveedores de servicios		
	Fabricantes de soluciones tecnológicas		
Grupo Modelo de Gobierno de Seguridad Informática			

Equipo de Implementación y Supervisión de Controles de seguridad Informática (EISC)	
Equipo de Respuesta a Incidentes	
RACI	**Participantes**
Aprobador	Director de Seguridad Informática
Responsable, Consultado e Informados	• Subdirector de Ciberseguridad • Subdirector de Cumplimiento de Seguridad Informática • Jefe de Departamento de Operación de Seguridad Informática • Profesional Operativo
Responsables y Consultados	• Centro de Atención a Usuarios (CAU) • Administradores de sistemas • Proveedores y/o fabricantes de soluciones tecnológicas
Funciones sustantivas	
• Seguimiento y revisión de las actividades propias para resolver una incidencia. • Asegurar la ejecución de las actividades y medidas preventivas o reactivas para la gestión de incidentes de seguridad informática, así como validar la eficacia de las de las acciones y cierre de los incidentes. • Ejecutar las actividades y medidas preventivas o reactivas para la gestión de incidentes de seguridad informática que permitan su resguardo y protección, a fin de mantener la continuidad de la operación y servicios de la SCJN, así como proteger la información frente a amenazas, internas o externas, deliberadas o accidentales, para asegurar el cumplimiento de la confidencialidad, integridad y disponibilidad de la información.	
Grupo Modelo de Gobierno de Seguridad Informática	
Equipo de Respuesta a Incidentes de Seguridad Informática (ERISC)	

Equipo de Gestión de Vulnerabilidades	
RACI	**Participantes**
Aprobador	Director de Seguridad Informática
Responsable, Consultado e Informados	• Subdirector de Ciberseguridad • Subdirector de Cumplimiento de Seguridad Informática • Jefe de Departamento de Operación de Seguridad Informática
Responsables y Consultados	• Administradores de sistemas • Usuarios/Clientes/Dueños
Funciones sustantivas	
• Seguimiento y revisión de las actividades propias para resolver una vulnerabilidad. • Asegurar la remediación de las vulnerabilidades identificadas, así como validar la eficacia de las de las acciones ejecutadas. • Analizar, aprobar, ejecutar y validar las actividades de remediación a las vulnerabilidades identificadas, así como justificar la no viabilidad de la remediación. • Cumplir con las políticas, disposiciones y procedimientos de seguridad informática. • Mantener la confidencialidad de contraseñas para el acceso a aplicaciones y sistemas de información. • Utilizar la información únicamente para los propósitos autorizados. • Participar en capacitaciones y programas de concientización en temas de seguridad informática. • Reportar cualquier incidente, potencial incidente u oportunidades de mejora identificadas.	

6 Planeación

6.1 Acciones para dirigir los riesgos y las oportunidades

La Política de Seguridad de la Información de la SCJN y sus políticas específicas correspondientes contemplan la evaluación del desempeño y eficacia del SGSI, incluyendo:

- Auditorías internas, la cual permite la planificación, establecimiento, implementación y mantenimiento de los programas de auditoría. Dichos programas toman en cuenta la importancia de los procesos involucrados y los resultados de las auditorías antecedentes.
- Revisiones por la dirección, que asegura la conveniencia, adecuación y eficacia continua del SGSI, describiendo el estado de acciones desde anteriores revisiones (cuando se cuente con el antecedente)
- No conformidades, acciones correctivas, oportunidades de mejora, que ayudan a conservar el nivel de cumplimiento de los objetivos de seguridad informática
- Evaluación y tratamiento del riesgo, que identifican, clasifican y atienden los puntos más sensibles de la operación para mitigar las consecuencias de las vulneraciones de seguridad en esta.

Cabe destacar que, la contribución activa y permanente a la seguridad informática de la SCJN otorga beneficios como el incremento de la confianza y satisfacción de las partes involucradas en la operación, el uso eficiente de los activos tecnológicos contra amenazas, así como el aumento de los niveles de sensibilidad, participación y motivación de los funcionarios de la SCJN respecto a la seguridad informática.

6.2 Objetivos del SGSI

La DSI ha establecido objetivos de seguridad informática que son congruentes con los objetivos y funciones mencionados en el Manual de Organización Específico – Dirección General de Tecnologías de la Información (MOE), apartado de Dirección de Seguridad Informática.

Además, estos objetivos pretenden dar cumplimiento a la Política de Seguridad de la Organización (ver 5.2 Política) y han sido creados con el fin de promover, mantener y mejorar las medidas de seguridad informática en la DSI.

Los objetivos del SGSI son:

1. Gestionar los riesgos de seguridad inherentes a los principales sistemas informáticos y sus activos relacionados de la DGTI y DSI de manera continua;
2. Atender y cerrar el mayor porcentaje de incidentes de seguridad informática registrados en la DGTI y DSI;
3. Establecer una cultura de seguridad de la información dentro de la DGTI y DSI;
4. Realizar revisiones periódicas sobre el cumplimiento de los controles de seguridad informática, y
5. Aplicar acciones preventivas, correctivas y de mejora a los resultados de la revisión.

Como parte del establecimiento del SGSI, para un mayor seguimiento al cumplimiento y logro de los objetivos se identificaron las siguientes actividades, recursos y responsables:

Objetivo	Actividades	Recursos	Responsable
Atender y cerrar el mayor porcentaje de incidentes de seguridad informática registrados en la DGTI y DSI.	Dar seguimiento y cerrar los incidentes de seguridad informática.	• Infraestructura, presupuesto, recurso humano.	DSI
Gestionar los riesgos de seguridad inherentes a los principales sistemas informáticos y sus activos relacionados de la DGTI y DSI de manera continua.	Realizar la identificación, análisis y tratamiento de riesgos por lo menos una vez al año.	• Inventario de Activos • Proceso de Gestión de Riesgos • Infraestructura, presupuesto, recurso humano.	DSI
Establecer una cultura de seguridad de la información dentro de la DGTI y DSI.	Implementar el programa de concientización.	• Programa de implementación. • Herramientas de concientización	DSI
Realizar revisiones periódicas sobre el cumplimiento de los controles de seguridad informática.	Realizar auditorías internas al SGSI de la DSI.	• Infraestructura, presupuesto, recurso humano.	DSI
Aplicar acciones correctivas y de mejora a los resultados de la revisión.	Aplicar acciones, preventivas, correctivas y de mejora a los resultados de la revisión.	• Infraestructura, presupuesto, recurso humano.	DSI

7 Soporte

7.1 Recursos

Es indispensable disponer de los recursos necesarios para la implementación y operación del SGSI de la SCJN según lo planeado.

En lo concerniente a la inversión económica, en términos generales se asignan los recursos presupuestales dispuestos para la DSI, de donde se desprende la contratación de los servicios de seguridad informática que cubran a toda la SCJN.

En ese orden de ideas es que se cuenta con instalaciones de la institución, de los proveedores, así como con los equipos específicos detallados en contratos y propios para proporcionar sistemas de defensa o detección de intrusiones en los sistemas de información y así mejorar los niveles de seguridad.

De igual forma, se cuenta con los perfiles y responsables del SGSI definidos (ver sección 5.3 Roles y Responsabilidades) y comunicados mediante el ejercicio de asignación de roles según sigue:

- Alta dirección
- Responsable del SGSI
- Responsable de Ciberseguridad
- Responsable de Gestión de riesgos
- Gestor de riesgos
- Responsable de respuesta a incidentes
- Gestor de respuesta a incidentes
- Responsable de gestión de vulnerabilidades
- Gestor de vulnerabilidades
- Gestor documental

7.2 Competencia

Con base en los procesos de la Dirección General de Recursos Humanos y el mecanismo del SGSI aplicable, se da cumplimiento con los requisitos de competencia del personal que lleva a cabo las tareas del SGSI, los cuales se centran en la competencia necesaria sobre la educación, capacitación y experiencia adecuadas al perfil de puesto formalizado y sus funciones establecidas en el Manual de Organización Específico. Se hace hincapié en la confiabilidad del personal que realice tareas sensibles para la SCJN en materia de ciberseguridad.

Asimismo, en la conformación del expediente se recopila y corrobora la información documental que soporta la competencia del personal interno en materia de seguridad informática. En caso de subcontratar servicios se establecen los perfiles específicos en los anexos técnicos correspondientes, los cuales deberán ser comprobados por el proveedor.

Las capacitaciones constantes, incluyendo las que forman parte del programa de concientización en materia de seguridad informática, también son el medio de asegurar y actualizar la competencia del personal interno y externo que cumpla plenamente con los objetivos propuestos.

Cabe mencionar que se prevé que todos los funcionarios y terceros con acceso a información sensible deben firmar acuerdos de confidencialidad o de no divulgación antes de que tengan los permisos para acceder a dicha información.

La concientización y capacitación de políticas de seguridad de la información deberá tomarse y evaluarse, como mínimo, de manera anual y deberá ser aprobado para considerar la capacitación como efectiva.

En las bajas de personal se deberá informar de la baja a la DGRH, custodiar y respaldar la información a la que tenía acceso el funcionario a fin de que no exista inconveniente al momento de la baja de sus accesos físicos y digitales.

7.3 Concienciación

En este requisito, básicamente se refiere a que los funcionarios que gestionan el SGSI deben conocer todo lo relacionado con las políticas y controles que lo conforman, lo cual se realiza a través de la notificación formal de sus roles y responsabilidades, comunicación permanente con el responsable del SGSI y la difusión de la política de seguridad del SGSI.

Asimismo, se cuenta con un programa de concientización con distintos módulos y evaluaciones utilizando todos los medios de comunicación al alcance de la DSI, incluyendo charlas presenciales, videoconferencias y las propias formaciones en la plataforma de concientización.

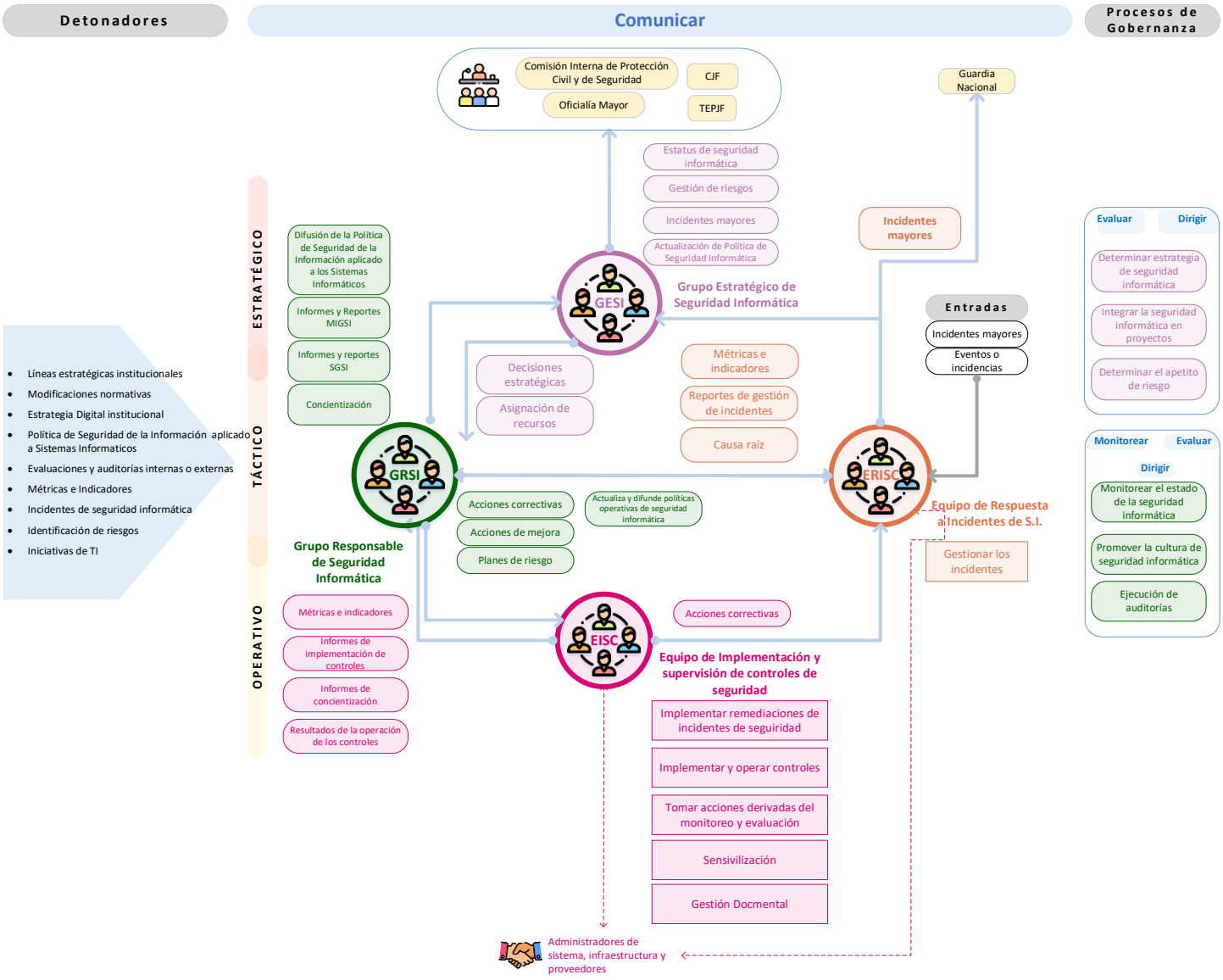
El responsable del SGSI mantiene informados a todos los involucrados sobre las actualizaciones en temas de seguridad, tomando en cuenta lo aprendido en los incidentes de seguridad y en los reportes de la prestación de servicios de ciberseguridad.

Lo anterior, sin dejar de contemplar la capacitación general a los funcionarios a fin de que todos sean conscientes de las funciones que se relacionan con el SGSI y cómo sus actividades afectan directamente a dichas funciones.

7.4 Comunicación

La DGTI, a través de la DSI, determina la necesidad de comunicaciones internas y externas relevantes para el SGSI, teniendo claro el objetivo por comunicar, cuándo, a quién y los procesos para dicha comunicación.

Se cuenta con el **Plan de comunicación** que describe funciones, roles y responsabilidades que describen las diferentes formas de comunicación, es decir, las reuniones formales de equipos de trabajo, además; describe los esquemas de comunicación permanente con los involucrados en el cumplimiento de controles de seguridad informática dentro del ámbito de sus responsabilidades, permitiendo ser más efectivos en la comunicación que coadyuva a la competencia como a la concienciación del personal.



7.5 Información Documentada

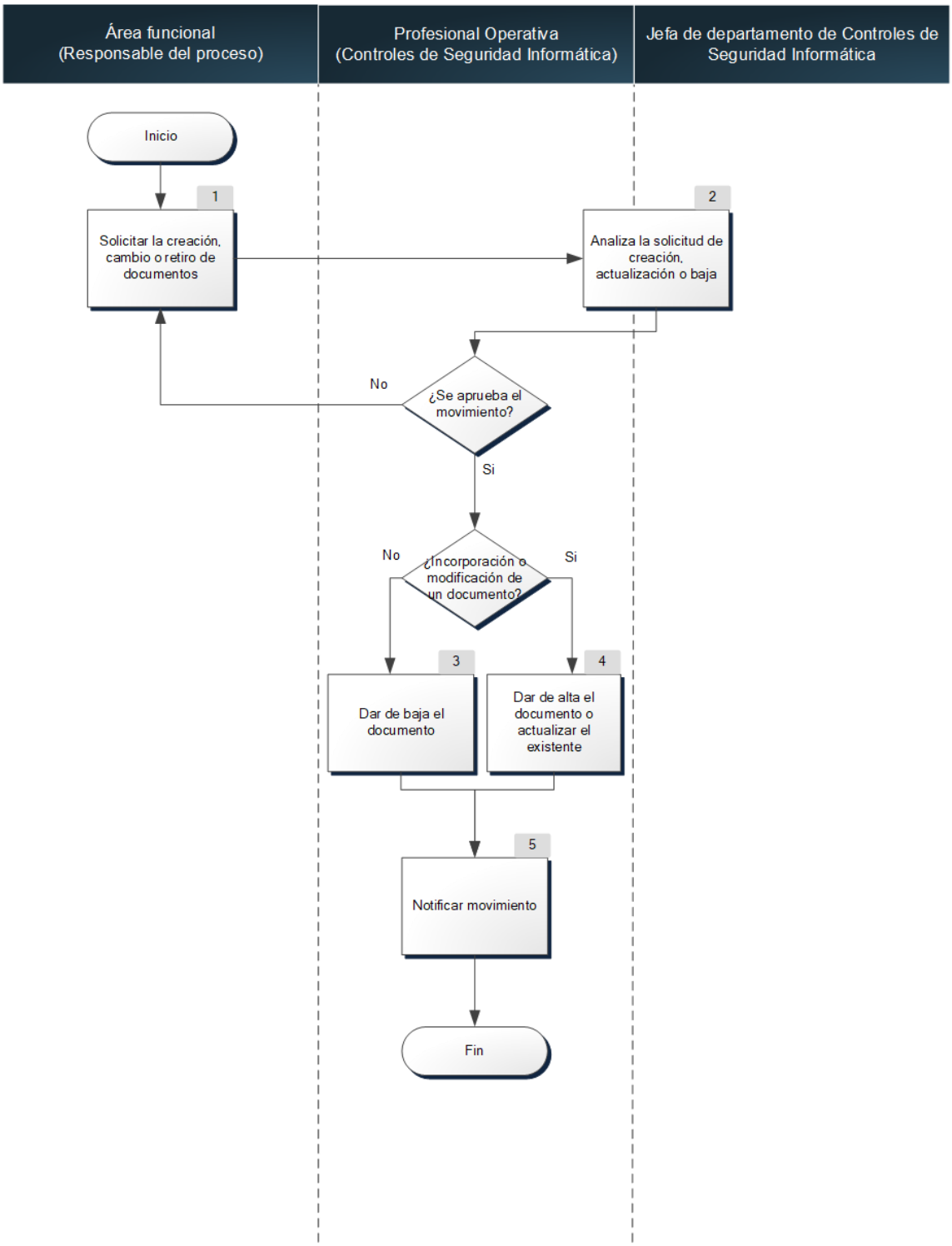
El SGSI de la DSI cuenta con información documentada que requiere el estándar internacional ISO/IEC 27001, que de manera enunciativa pero no limitativa se establece:

- **Manual del Sistema de Gestión de Seguridad de la Información;**
  - Código: MAN-SGSI-01
  - Alcance: DSI
  - Objetivo: Definir el marco gestor y aspectos particulares de la seguridad informática en la SCJN, con base en estándares internacionales y mejores prácticas, congruentes con la política de seguridad informática, la misión y visión de la SCJN, con el fin de promover, mantener y mejorar las medidas de seguridad informática institucionales.

- Contenido solicitado por el estándar:
  - Política del Sistema de Gestión de Seguridad de la Información (ver sección 5.2 Política)
  - Alcance del Sistema de Gestión de Seguridad de la Información (ver sección 4.3 Alcance del Sistema de Gestión de Seguridad de la Información)
  - Roles y Responsabilidades (ver sección 5.3 Roles y Responsabilidades)

- **Procedimiento de Gestión del Control Documental**
  - Código: PSI-SGSI-06
  - Alcance: DSI
  - Objetivo: Establecer las especificaciones necesarias para la identificación, elaboración, revisión, aprobación, organización, disposición o actualización de los documentos del Sistema de Gestión de la Seguridad Informática de la Dirección de Seguridad de la Información.

    - Ciclo de creación y actualización en el cual se establecen las especificaciones necesarias para la identificación, elaboración, revisión, aprobación, organización, emisión, disposición y actualización de los documentos internos de la DSI:



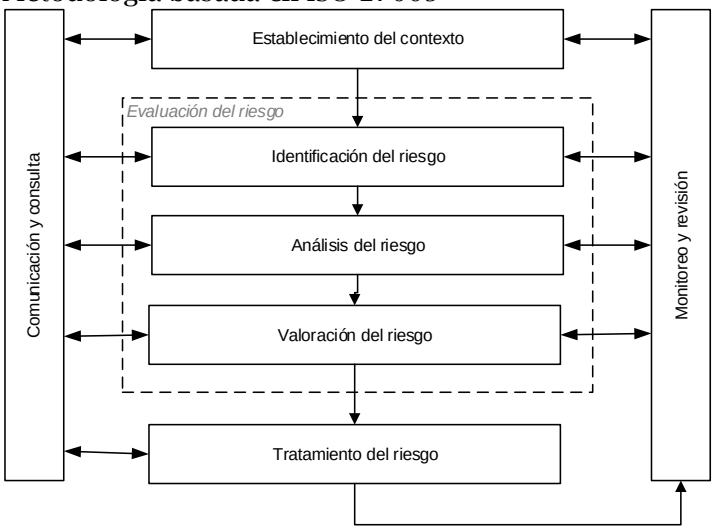
- Control de la información documentada:

La información documentada que se elabora como necesidad del SGSI y de la naturaleza de las operaciones de la DSI se encuentra disponible en el repositorio documental que establezca la dirección.

La DSI ha designado el rol de **Gestor Documental**, con la finalidad de que solo una persona tenga acceso a los documentos editables de la información y que esta misma pueda tener el control documental respecto a la versión, fecha de creación y clasificación del documento, así como la difusión de la información.

A través del uso de la Lista Maestra de documentos, el Gestor Documental puede gestionar el control de la información de la DSI.

- **Procedimiento de Gestión de Riesgos**
  - Código: PSI-SGSI-07 (ver sección 8 Operación)
  - Alcance: DGTI / DSI
  - Objetivo: Identificar, analizar, evaluar y controlar los riesgos de seguridad de la información como parte del Modelo Institucional de Gobierno de Seguridad de la Información (MIGSI) y del Sistema de Gestión de Seguridad de la Información (SGSI) en función al alcance establecido.
  - Contenido relevante:
    - Metodología basada en ISO 27005



    - Fuentes de información:
      - Entrevistas con personal
      - Análisis de resultados de reportes
      - Consulta de fuentes de información externas
      - Consulta de repositorios internos
      - Reportes de herramientas automatizadas
      - Información histórica de la DGTI
      - Información histórica generada por el COC
      - Información histórica generada por el área de ciberinteligencia

- Información histórica generada por el área de análisis de vulnerabilidades

▪ Criterios para la determinación del nivel de riesgo:
- Criterios para la identificación de activos
- Criterios para la identificación de la criticidad de los activos
- Criterios para la identificación de amenazas
- Catálogo de agentes de amenaza y amenazas
- Criterios para la determinación de escenarios de riesgo
- Criterios para la identificación de vulnerabilidades
- Catálogo de vulnerabilidades
- Criterios para la identificación de la probabilidad de ocurrencia de un riesgo
- Evaluación de la probabilidad
- Criterios para la identificación del impacto potencial
- Criterios para la valoración del riesgo

- **Declaración de aplicabilidad (SoA)**
  - Código: SoA-SGSI-01
  - Alcance: DGTI / DSI
  - Objetivo: Identificar los controles de seguridad informática que son aplicables en el marco del SGSI y del MIGSI, considerando su alcance y actividades esenciales, con base en los controles que indica el Anexo A del estándar internacional ISO/IEC 27001:2013.

- **Procedimiento de Auditoría**
  - Código: PSI-SGSI-10 (ver sección 9.2 Auditoría Interna)
  - Alcance: DSI
  - Objetivo: Detallar y precisar, de forma sistemática, las actividades para la elaboración, implementación y ejecución de programas de auditoría que permitan a la DSI obtener información para la toma de decisiones que contribuyan al cumplimiento y mejora del SGSI.

- **Procedimiento de Mejora**
  - Código: PSI-SGSI-11 (ver sección 10.2 Mejora continua)
  - Alcance: DSI
  - Objetivo: Describir las actividades para mejorar de manera continua la idoneidad, adecuación y eficacia del SGSI.

- **Procedimiento de Acciones correctivas**
  - Código: PSI-SGSI-12 (ver sección 10.1 Acciones correctivas)
  - Alcance: DSI

- Objetivo: Describir las actividades para registrar las no conformidades, llevar a cabo las acciones correctivas aplicables, así como utilizar las oportunidades de mejora con la finalidad de garantizar la idoneidad, adecuación y eficacia del SGSI.

Para efectos de la operación de los servicios de seguridad informática de la DSI, se cuentan con los procesos documentados mencionados en numeral 4. Contexto de la organización y que son:

- **Procedimiento para el Análisis de Vulnerabilidades de la Infraestructura Tecnológica de Aplicaciones de la SCJN**
  - Código: PO-TI-SI-01
  - Alcance: DGTI / DSI
  - Objetivo: Realizar la detección temprana de vulnerabilidades informáticas en la infraestructura tecnológica de aplicaciones de este Alto Tribunal, con el propósito de prevenir y disminuir fallas de seguridad del aplicativo que, en caso de ser explotadas, podrían comprometer la integridad, disponibilidad y confidencialidad de la información de este Alto Tribunal.

- **Procedimiento para el Análisis Forense Informático**
  - Código: PO-TI-SI-02
  - Alcance: DGTI / DSI
  - Objetivo: Realizar el proceso para la obtención, preservación y documentación de evidencia digital en equipos o dispositivos de cómputo de usuario o de servidores de datos, para determinar las causas que han originado un incidente de seguridad informática o una vulneración a la confidencialidad, integridad o disponibilidad de la información de alguna de las áreas de la Suprema Corte de Justicia de la Nación.

- **Procedimiento para la Administración de Borrado Seguro en Dispositivos Informáticos**
  - Código: PO-TI-SI-03
  - Alcance: DGTI / DSI
  - Objetivo: Realizar el borrado seguro de la información en las unidades de almacenamiento de los equipos de cómputo institucionales (servidores y equipos de usuario) que sean solicitados por escrito a la Dirección de Seguridad Informática, a fin de preservar la confidencialidad de la información al evitar que la misma pueda ser recuperada en el futuro por otro usuario del mismo equipo.

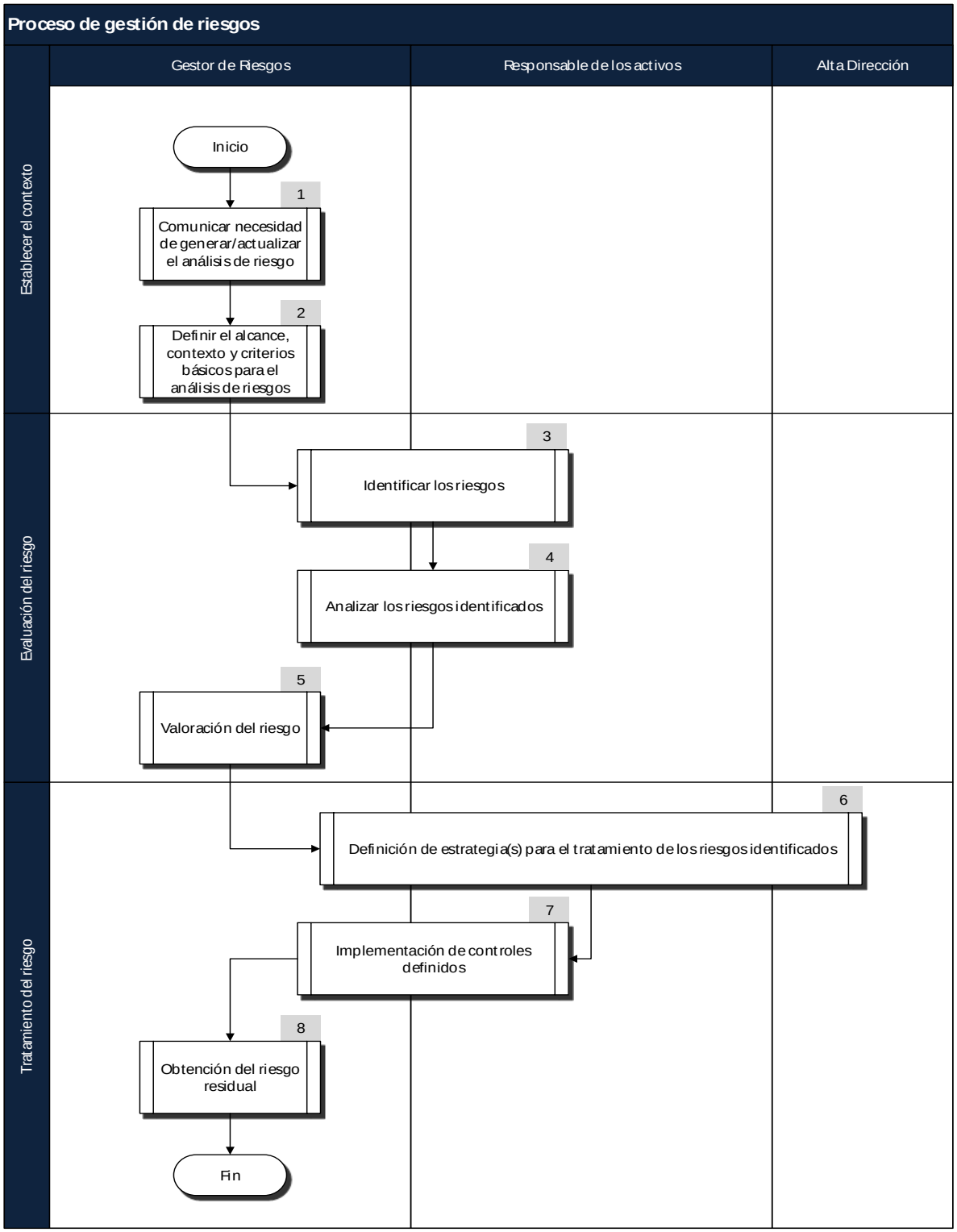
- **Procedimiento para la Administración de Políticas de Seguridad Perimetral y de Filtrado de Contenido**
  - Código: PO-TI-SI-04
  - Alcance: DGTI / DSI
  - Objetivo: Gestionar las políticas de los dispositivos de seguridad perimetral y de filtrado de contenido, con el objeto de hacer un uso más seguro y eficiente del acceso y publicación hacia internet, así como gestionar los accesos a los servicios de las redes internas LAN/WAN por parte de los usuarios de la Suprema Corte de

Justicia de la Nación, para establecer una mayor protección contra flujos de red y protocolos inseguros.

- **Procedimiento de Respuesta a Incidentes de Seguridad Informática**
  - Código: PO-TI-SI-05
  - Alcance: DGTI / DSI
  - Objetivo: Establecer los criterios, mecanismos y acciones para identificar, atender y dar seguimiento a los incidentes de seguridad informática para contener el impacto que estos puedan ocasionar en la infraestructura tecnológica de la Suprema Corte de Justicia de la Nación.
  - Anexos:
    - Anexo 1: Protocolo de Atención a Incidentes Mayores
      - Objetivo: Establecer un protocolo de atención para los incidentes mayores de seguridad informática, en alineación con las mejores prácticas identificadas en el Protocolo Nacional Homologado de Gestión de Incidentes Cibernéticos, a fin de lograr niveles de riesgo aceptables y contribuir al logro de los objetivos de la SCJN.

8 Operación

La DSI ha establecido el **Procedimiento de Gestión de Riesgos (PSI-SGSI-07)**, con el objetivo de identificar, analizar, evaluar y controlar los riesgos de seguridad de la información como parte del Modelo Institucional de Gobierno de Seguridad de la Información (MIGSI) y del Sistema de Gestión de Seguridad de la Información (SGSI) en función al alcance establecido.

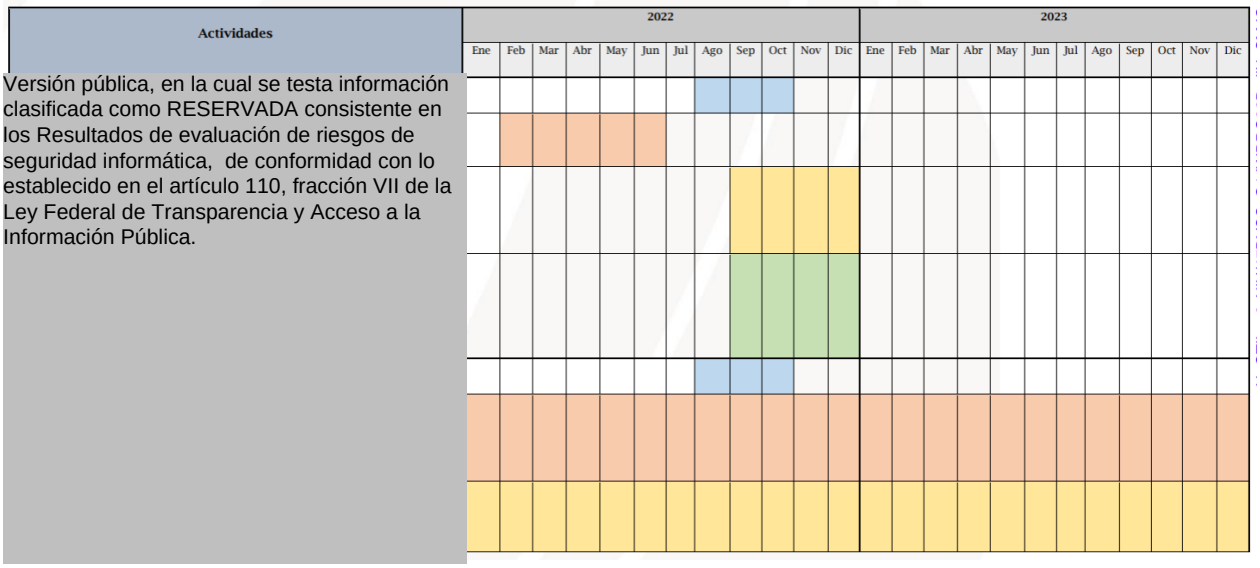

Proceso de gestión de riesgos
Gestor de Riesgos
Responsable de los activos
Alta Dirección
Establecer el contexto
Evaluación del riesgo
Tratamiento del riesgo
Inicio
1
Comunicar necesidad de generar/actualizar el análisis de riesgo
2
Definir el alcance, contexto y criterios básicos para el análisis de riesgos
3
Identificar los riesgos
4
Analizar los riesgos identificados
5
Valoración del riesgo
6
Definición de estrategia(s) para el tratamiento de los riesgos identificados
7
Implementación de controles definidos
8
Obtención del riesgo residual
Fin

Dicho método se basa en las buenas prácticas establecidas en el estándar ISO 27005, además el procedimiento documentado considera los siguientes puntos para determinar el nivel de riesgo:

1. Fuentes de información para la ejecución del ejercicio de gestión de riesgos
2. Criterios para la identificación de activos
3. Criterios para la identificación de la criticidad de los activos
4. Criterios para la identificación de amenazas
5. Catálogo de agentes de amenaza y amenazas
6. Criterios para la determinación de escenarios de riesgo
7. Criterios para la identificación de vulnerabilidades
8. Catálogo de vulnerabilidades
9. Criterios para la identificación de la probabilidad de ocurrencia de un riesgo
10. Evaluación de la probabilidad
11. Criterios para la identificación del impacto potencial
12. Criterios para determinar el nivel de riesgo
13. Criterios para la valoración del riesgo
14. Respuesta al riesgo

El ejercicio de análisis de riesgo se actualizará al menos una vez al año o cuando la alta dirección así lo considere necesario.

El resultado del ejercicio se presenta a los Dueños o Administradores de los sistemas críticos (Consultar la sección “Anexo 2 Ejercicio de Análisis de Riesgos”), para que se determine la respuesta al riesgo que se dará y se realice el Plan de Tratamiento de riesgos:



9 Evaluación del desempeño

La evaluación del desempeño del SGSI de la SCJN dará pie a la revisión por parte de la dirección, conteniendo no conformidades y acciones correctivas, seguimiento y medición de resultados, cumplimiento de objetivos de seguridad de la información y oportunidades de mejora.

9.1 Indicadores clave de desempeño (KPIs)

Resulta imprescindible contar con un esquema de indicadores que permita analizar y medir qué impacto, repercusión y resultado ha tenido cada una de las acciones que se han tomado y llevado a cabo.

Los indicadores del SGSI aportan visibilidad imprescindible para conocer si los comportamientos individuales de políticas, controles, procedimientos, etc., están alineados a los objetivos del SGSI, en términos de actividad y eficiencia.

Los indicadores fueron definidos en vinculación directa con los objetivos del SGSI y de su política de seguridad informática, lo que representa trazabilidad y correspondencia con lo establecido como parte de las disposiciones y esquema del SGSI. (ver punto 6.1. Objetivos del SGSI).

El modelo de indicadores del SGSI de la SCJN se establece con base en la Metodología de Marco Lógico, en consideración directa a los objetivos de seguridad informática y medios de verificación para la generación de dichos indicadores.

Los principales aspectos susceptibles de monitoreo, en la fase de implementación e inicio de operación del SGSI son todas las evidencias documentales generadas, debiendo ser formalizados mediante las firmas correspondientes y puestos a disposición del personal o proveedores junto con el proceso de concientización, capacitación y difusión correspondiente, generando y ordenando las evidencias de dichas acciones, diferenciando los repositorios de información a fin de facilitar los procesos de revisión documental en las evaluaciones posteriores.

En el caso específico del SGSI de la SCJN, las métricas e indicadores fueron definidas en vinculación directa con los objetivos del SGSI y de su política de seguridad informática, lo que representa trazabilidad y correspondencia con lo establecido como parte de las disposiciones y esquema del SGSI.

La descripción de los indicadores corresponde a lo siguiente:

Objetivo vinculado	Nombre del indicador
Atender y cerrar el mayor porcentaje de incidentes de seguridad informática registrados en la DGTI y DSI.	**Incidencias de seguridad informática resueltas**
Gestionar los riesgos de seguridad inherentes a los principales sistemas informáticos y sus activos relacionados de la DGTI y DSI de manera continua.	**Riesgos tratados**
	Vulnerabilidades críticas atendidas
Establecer una cultura de seguridad de la información dentro de la DGTI y DSI.	**Concientización en seguridad informática**
Realizar revisiones periódicas sobre el cumplimiento de los controles de seguridad informática.	**Controles de seguridad informática**
	Controles de seguridad
Aplicar acciones correctivas y de mejora a los resultados de la revisión.	**Atención a hallazgos derivados de revisión de controles**

9.2 Auditoría interna

El procedimiento de Auditoría Interna (PSI-SGSI-10) del SGSI detalla, de forma sistemática, las actividades para la elaboración, implementación y ejecución de programas de auditoría que permitan a la DSI obtener información para la toma de decisiones que contribuyan al cumplimiento y mejora del SGSI.

Dicho proceso es aplicable para el personal de la SCJN involucrado en las auditorías internas al SGSI de la SCJN, dentro del marco de procesos, controles y servicios de la DSI, incluyendo los principios de la auditoría, gestión de los programas de auditoría, así como en la evaluación de la competencia de los individuos que participen en el proceso, auditores y equipos de trabajo que culmine en la información útil a la DSI y la documentación correspondiente.

Las actividades del proceso corresponden a lo siguiente:

1. Establecer objetivos del programa de auditoría.

    a. Definir objetivos del programa de auditorías.
    b. Establecer el alcance y dimensión del programa de auditorías.

2. Determinar y evaluar los riesgos y oportunidades del programa de auditoría.

    a. Considerar los riesgos asociados a la planificación, a los recursos, selección del equipo auditor, a la implementación, registros y controles, así como al seguimiento, revisión y mejora del programa de auditoría.

3. Establecer el programa de auditoría.

    a. Establecer funciones y competencias de los responsables de gestionar el programa y cada una de las auditorías.
    b. Determinar alcance, duración y calendario de auditorías.
    c. Establecer el procedimiento a seguir en las auditorías (definir criterios y métodos).
    d. Identificar y asignar los recursos (selección y evaluación del equipo).

4. Implementar el programa de auditoría.

    a. Gestionar la ejecución del programa de auditoría.

5. Dar seguimiento al programa de auditoría.

    a. Dar seguimiento y evaluar la ejecución del programa.
    b. Analizar y revisar la efectividad de las actividades realizadas como parte de la auditoría.
    c. Evaluar a los equipos auditores.
    d. Retroalimentar al equipo auditor.
    e. Modificar el programa de ser necesario.

6. Revisar y mejorar el programa de auditoría.

    a. El auditor líder deberá medir y evaluar el cumplimiento de objetivos del programa de auditoría.

b. El auditado deberá analizar resultados finales e identificar áreas de oportunidad y de mejora.
c. El auditado deberá mejorar de manera continua el programa para futuras auditorías.

7. Iniciar la auditoría.

a. El equipo auditor deberá hacer contacto inicial con el responsable del proceso a auditar.
b. El auditor líder deberá presentar objetivos, alcance, método y al equipo auditor.
c. El auditado y auditor líder deberán determinar la viabilidad de la auditoría (información, tiempo y recursos).

8. Preparar las actividades de auditoría.

a. El auditado deberá reunir información y documentos de trabajo del proceso por auditar.
b. El auditado y equipo auditor deberán establecer y priorizar las actividades a seguir en la auditoría.
c. El auditor líder deberá elaborar el plan de auditoría (detalle y agenda) basado en el programa de auditoría y la información proporcionada por el auditado.
d. El auditor líder deberá determinar alcance, duración de actividades y agenda de auditorías.
e. El auditor líder deberá asignar tareas al equipo auditor.
f. El auditado y equipo auditor deberán preparar las listas de verificación, planes de muestreo y formularios para registro de información.
g. El auditado y equipo auditor deberán recuperar auditorías previas sólo en caso de ser necesario tomar algún resultado o hallazgo previo como antecedente.

9. Realizar las actividades de auditoría.

a. El auditor líder deberá realizar la reunión de apertura para confirmar el acuerdo de todas las partes (equipo auditor y auditado) y presentar al equipo auditor.
b. El auditor líder deberá presentar el plan de auditoría para confirmar los acuerdos entre las partes y asegurar que se pueden realizar las actividades planificadas.
c. El auditado y equipo auditor deberán recopilar evidencia y verificar contra los criterios de auditoría establecidos mediante las técnicas que se consideren apropiado (entrevistas, observaciones, documentos, etc.)
d. El auditor líder deberá reunir al equipo auditor de manera periódica para intercambiar información, evaluar el progreso de la auditoría y reasignar tareas.
e. El auditor líder deberá celebrar reuniones con el auditado de manera periódica para comunicar el avance de la auditoría, cambios y hallazgos que requieran atención inmediata.
f. El equipo auditor deberá determinar los hallazgos, conclusiones y recomendaciones de la auditoría.
g. El equipo auditor deberá revisar los hallazgos con el auditado (conformidad o no conformidad), como cierre parcial, al término de cada auditoría individual.
h. El auditado y equipo auditor deberán realizar reunión de cierre con los representantes del Auditado y, en su caso, responsables de funciones o procesos auditados.

10. Preparar y distribuir el informe de auditoría.

    a. Registrar en el informe, de manera completa, precisa, concisa y clara, el desarrollo y resultados de la auditoría de acuerdo con los procedimientos del programa de auditoría.
    b. En el periodo acordado, el informe deberá emitirse fechado, revisado y aprobado.
    c. Distribuir el informe a los receptores por parte del Auditado.
    d. Finalizar la auditoría.
    e. Conservar o destruir los documentos de la auditoría de común acuerdo entre equipo auditor y auditado.
    f. Incorporar, en su caso, las lecciones aprendidas de la auditoría al proceso de mejora continua del SGSI.

11. Realizar las actividades de seguimiento a la auditoría.

    a. Analizar, en conjunto, las conclusiones de la auditoría susceptibles de generar acciones correctivas, preventivas o de mejora.
    b. El auditado deberá ejecutar las acciones correctivas, preventivas o de mejora determinadas, de acuerdo con los intervalos de tiempo establecidos.
    c. El auditado deberá mantener informado al equipo auditor cuando sea pertinente acerca del estado de las acciones antes mencionadas

9.3 Revisión por la dirección

La alta dirección de la DSI deberá revisar el sistema de gestión conforme a lo dispuesto en los procesos que forman parte del SGSI.

Dichas revisiones consideran los resultados de ejercicios de revisión previos, cambios en cuestiones internas y externas que afecten al SGSI, así como el comportamiento del SGSI derivado de no conformidades y acciones correctivas tal y como se describe en el proceso de auditoría, el seguimiento y resultado de mediciones derivado de los indicadores clave de desempeño, además de las oportunidades identificadas como se refleja en el proceso de mejora y los resultados del tratamiento de riesgos.

Al final de cualquier proceso de planeación, ejecución y evaluación del SGSI deberá arrojar decisiones por parte de la dirección, relacionadas con la mejora y necesidades de cambio del SGSI que permitan cumplir con sus objetivos, generando y documentando los acuerdos de los temas presentados.

10 Mejora

El tema de control de acciones correctivas y de mejora continua, junto con lo correspondiente al tema de mejora dispuesto en las políticas específicas del SGSI de la SCJN, describe los pasos a seguir para reaccionar ante las no conformidades, lo que permitirá llevar a cabo las acciones para controlarla y corregirla, así como hacer frente a las consecuencias.

De igual forma, se definirán los pasos para evaluar la necesidad de acciones para eliminar las causas de no conformidades, revisándolas, determinando dichas causas y si existen potenciales no conformidades.

La DSI tiene documentado el proceso integral de mejora continua, considerando la idoneidad, adecuación y eficacia del SGSI.

10.1 Acciones correctivas

El procedimiento de Acciones Correctivas (PSI-SGSI-12) del SGSI de la SCJN describe las actividades para registrar las no conformidades, llevar a cabo las acciones correctivas aplicables, así como utilizar las oportunidades de mejora con la finalidad de garantizar la idoneidad, adecuación y eficacia del SGSI.

Dicho proceso es aplicable para el personal de la SCJN involucrado en la atención de no conformidades en la operación del SGSI de la SCJN, mediante la ejecución de acciones correctivas dentro del marco de procesos, controles y servicios de la DSI, asegurando la documentación correspondiente.
Las actividades del proceso corresponden a lo siguiente:

1. Identificar no conformidades u oportunidades de mejora.

    a. Identificar no conformidades y oportunidades de mejora, información derivada de indicadores de gestión, revisión de la dirección y auditorías.

2. Registrar no conformidades u oportunidades de mejora.

    a. Registrar las no conformidades y oportunidades de mejora en el informe de no conformidades.
    b. Analizar y discriminar la no conformidad.
    c. Revisar si se puede reprocesar para documentar dicho reproceso.
    d. Revisar si se desecha para impedir la continuación del servicio y se documenta.

3. Analizar no conformidades u oportunidades de mejora

    a. Analizar e identificar la causa raíz a través de los cinco por qué o diagrama de causa efecto.

4. Determinar acciones correctivas.

    a. Definir planes de acción, considerando parámetros como frecuencia en que la desviación se ha presentado, impacto relacionado a los objetivos esperados, así como criterios y opiniones de los dueños de procesos y actividades del SGSI.
    b. Determinar las acciones de corrección inmediata para evitar que la desviación genere en mayor impacto.
    c. El Responsable del SGSI registrará las acciones necesarias para eliminar la causa raíz detectada.
    d. Las acciones deben describir el detalle de las actividades a realizar, así como el tiempo requerido, responsables y recursos asignados.
    e. Las actividades deben considerar una adecuación del sistema, procesos, actividades o productos, según sea conveniente.

f. Debe considerarse el tiempo requerido para la implantación y madurez de las acciones, con el propósito de lograr observar su efectividad.

5. Ejecutar acciones correctivas.

   a. Ejecutar o coordinar la ejecución de las acciones de remediación necesarias.
   b. Documentar, revisar y, en su caso, validar que la evidencia presentada es consistente y congruente con las acciones determinadas.

6. Dar seguimiento y cierre de acciones correctivas.

   a. Llevar a cabo el seguimiento y cierre de las acciones correctivas y oportunidades de mejora.
   b. Coordinar la revisión de eficacia de todas las acciones implementadas.
   c. Revisar los resultados y presentarlos a la alta dirección.
   d. En el caso de que se compruebe que la acción ha sido efectiva, ésta se considera como cerrada y se registra en el reporte de acciones correctivas.
   e. Si no se valida la efectividad de la acción, solicitan al responsable que revise y adecúe lo necesario para lograr la efectividad requerida.
   f. Ninguna acción correctiva o preventiva puede considerarse como cerrada hasta en tanto no demuestre efectividad.
   g. El control y seguimiento de acciones correctivas deberá incluir fecha de detección, proceso o área, fuente, causa, responsable del cierre y fechas compromiso.

10.2 Mejora continua

El proceso de mejora del SGSI de la SCJN describe las actividades para mejorar de manera continua la idoneidad, adecuación y eficacia del SGSI, acciones aplicables para el personal de la SCJN responsable e involucrado en la mejora del SGSI.

Las actividades del proceso corresponden a lo siguiente:

1. Identificar oportunidades de mejora.

   a. Identificar oportunidades de mejora derivadas de indicadores de gestión o de desempeño, revisión de la dirección y/o no conformidades derivadas de auditorías.

2. Determinar y registrar acciones de mejora.

   a. Analizar y determinar las acciones de mejora aplicables.
   b. Registrar las oportunidades de mejora en el plan de mejora.
   c. Dicho plan deberá contener, como mínimo, identificador de las acciones de mejora, descripción, responsable, recursos asignados y fechas compromiso.
   d. Tomar en cuenta criterios y opiniones de los dueños de procesos y actividades del SGSI.
   e. Las actividades que incluyan adecuación del sistema, procesos, actividades o productos, deberán realizarse considerando el control de cambios del SGSI.

3. Ejecutar acciones de mejora.

    a. Considerar el tiempo requerido para la implantación y madurez de las acciones de mejora con el propósito de lograr observar su efectividad.
    b. Ejecutar o coordinar la ejecución de las acciones de mejora.
    c. Documentar, revisar y, en su caso, validar que la evidencia presentada es consistente y congruente con las acciones ejecutadas.

4. Dar seguimiento y cerrar acciones de mejora.

    a. Llevar a cabo el seguimiento y cierre de las acciones de mejora.
    b. Coordinar la revisión de eficacia de todas las acciones implementadas.
    c. Revisar los resultados y presentarlos a la alta dirección.
    d. En el caso de que se compruebe que la acción ha sido efectiva, ésta se considera como cerrada y se registra en el plan de mejora como cierre de acciones de mejora.
    e. Si no se valida la efectividad de la acción, solicitar al responsable que revise y adecúe lo necesario para lograr la efectividad requerida.

Anexos

- **Anexo 1. Indicadores clave de desempeño del SGSI**

Sistema de Gestión de Seguridad de la Información							
Indicadores							
Nombre del indicador	**Objetivo vinculado**	**Definición o descripción**	**Fórmula**	**Unidad de medida**	**Periodicidad**	**Responsable del indicador**	**Meta**
Incidencias de seguridad informática resueltas	Atender y cerrar el mayor porcentaje de incidentes de seguridad informática registrados en la DGTI y DSI.	**Mide la eficiencia de incidentes atendidos**	Eficiencia la atención de incidentes = (# de incidentes cerrados / # de incidentes registrados durante el periodo) x100	Porcentaje	Mensual	DSI	>=96%
Riesgos tratados	Atender los riesgos identificados en función al apetito de riesgo establecido.	**Mide el porcentaje de riesgos atendidos**	% de riesgos gestionados = ((# de riesgos identificados con plan de tratamiento) / (# de riesgos identificados)) x100	Porcentaje	Semestral	DSI	>=80%
Vulnerabilidades críticas atendidas	Gestionar los riesgos de seguridad inherentes a los principales sistemas informáticos y sus activos relacionados de la	**Mide el porcentaje de vulnerabilidades críticas tratadas**	% de vulnerabilidades críticas tratadas = ((# de vulnerabilidades con severidad alta resueltas) / (# de vulnerabilidades con severidad alta identificadas)) x100	Porcentaje	Semestral	DSI	>=90%

	DGTI y DSI de manera continua.						
Concientización en seguridad informática	Identificar la eficiencia de la difusión de la concientización.	**Mide la efectividad del programa de concientización**	% de efectividad sobre la cultura de SI = (# personas que obtuvieron la constancia / # que ingresaron a la herramienta y cursaron por lo menos el primer módulo) x 100	Porcentaje	Mensual	DSI	Por definir en función a los históricos recolectados (ejercicio 2023)

Sistema de Gestión de Seguridad de la Información							
Indicadores							
Nombre del indicador	**Objetivo vinculado**	**Definición o descripción**	**Fórmula**	**Unidad de medida**	**Periodicidad**	**Responsable del indicador**	**Meta**
Controles de seguridad informática	Realizar revisiones periódicas sobre el cumplimiento de los controles de seguridad informática.	**Mide los controles implementados en su totalidad contra los establecidos para adoptar por parte de la SCJN**	% de controles implementados = (Número de controles implementados en su totalidad o actualizados / Número de controles establecidos) x 100	Porcentaje	Bimestral	DSI	Por definir en función a los históricos recolectados (ejercicio 2023)

Atención a hallazgos derivados de revisión de controles	Aplicar acciones preventivas, correctivas y de mejora a los resultados de la revisión.	**Mide el porcentaje de acciones aplicadas derivadas de las revisiones a los controles declarados**	% de acciones aplicadas = ((# de acciones preventivas/correctivas/mejoras aplicadas) / (# de hallazgos encontrados)) x100	Porcentaje	Semestral	DSI	Por definir en función a los históricos recolectados (ejercicio 2023)
Revisiones al SGSI	Realizar revisiones periódicas sobre el cumplimiento de los controles de seguridad informática.	**Comprueba que las revisiones planeadas sean ejecutadas**	% de revisiones realizadas = ((# de revisiones realizadas) / (# de revisiones planeadas)) x100	Porcentaje	Anual	DSI	Por definir en función a los históricos recolectados (ejercicio 2023)

- **Anexo 2. Gestión del riesgo**
  - **Resultados del análisis de riesgo**

El ejercicio de gestión de riesgos nos deja ver el nivel de protección que tiene cada uno de los sistemas considerados críticos para la SCJN y, además, ayuda a identificar brechas de seguridad que pueden ser aprovechadas por una o varias amenazas.

Versión pública, en la cual se testa información clasificada como RESERVADA consistente en los Resultados de evaluación de riesgos de seguridad informática, de conformidad con lo establecido en el artículo 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública.

#	Vulnerabilidad	Amenaza	Nivel de protección del sistema	Grado de exposición	Evaluación de probabilidad	Evaluación de impacto	Valor del riesgo	Nivel de riesgo

Versión pública, en la cual se testa información clasificada como RESERVADA consistente en los Resultados de evaluación de riesgos de seguridad informática, de conformidad con lo establecido en el artículo 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública.

#	Vulnerabilidad	Amenaza	Nivel de protección del sistema	Grado de exposición	Evaluación de probabilidad	Evaluación de impacto	Valor del riesgo	Nivel de riesgo

Versión pública, en la cual se testa información clasificada como RESERVADA consistente en los Resultados de evaluación de riesgos de seguridad informática, de conformidad con lo establecido en el artículo 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública.

#	Vulnerabilidad	Amenaza	Nivel de protección del sistema	Grado de exposición	Evaluación de probabilidad	Evaluación de impacto	Valor del riesgo	Nivel de riesgo

Versión pública, en la cual se testa información clasificada como RESERVADA consistente en los Resultados de evaluación de riesgos de seguridad informática, de conformidad con lo establecido en el artículo 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública.

Establecimiento de los riesgos:

Versión pública, en la cual se testa información clasificada como RESERVADA consistente en los Resultados de evaluación de riesgos de seguridad informática, de conformidad con lo establecido en el artículo 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública.

Versión pública, en la cual se testa información clasificada como RESERVADA consistente en los Resultados de evaluación de riesgos de seguridad informática, de conformidad con lo establecido en el artículo 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública.

Versión pública, en la cual se testa información clasificada como RESERVADA consistente en los Resultados de evaluación de riesgos de seguridad informática, de conformidad con lo establecido en el artículo 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública.

Versión pública, en la cual se testa información clasificada como RESERVADA consistente en los Resultados de evaluación de riesgos de seguridad informática, de conformidad con lo establecido en el artículo 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública.

Versión pública, en la cual se testa información clasificada como RESERVADA consistente en los Resultados de evaluación de riesgos de seguridad informática, de conformidad con lo establecido en el artículo 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública.

Versión pública, en la cual se testa información clasificada como RESERVADA consistente en los Resultados de evaluación de riesgos de seguridad informática, de conformidad con lo establecido en el artículo 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública.

#	Vulnerabilidad	Amenaza	Nivel de protección del sistema	Grado de exposición	Evaluación de probabilidad	Evaluación de impacto	Valor del riesgo	Nivel de riesgo

Versión pública, en la cual se testa información clasificada como RESERVADA consistente en los Resultados de evaluación de riesgos de seguridad informática, de conformidad con lo establecido en el artículo 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública.

#	Vulnerabilidad	Amenaza	Nivel de protección del sistema	Grado de exposición	Evaluación de probabilidad	Evaluación de impacto	Valor del riesgo	Nivel de riesgo

Versión pública, en la cual se testa información clasificada como RESERVADA consistente en los Resultados de evaluación de riesgos de seguridad informática, de conformidad con lo establecido en el artículo 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública.

Establecimiento de los riesgos:

Versión pública, en la cual se testa información clasificada como RESERVADA consistente en los Resultados de evaluación de riesgos de seguridad informática, de conformidad con lo establecido en el artículo 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública.

Versión pública, en la cual se testa información clasificada como RESERVADA consistente en los Resultados de evaluación de riesgos de seguridad informática, de conformidad con lo establecido en el artículo 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública.

Versión pública, en la cual se testa información clasificada como RESERVADA consistente en los Resultados de evaluación de riesgos de seguridad informática, de conformidad con lo establecido en el artículo 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública.

Versión pública, en la cual se testa información clasificada como RESERVADA consistente en los Resultados de evaluación de riesgos de seguridad informática, de conformidad con lo establecido en el artículo 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública.

Versión pública, en la cual se testa información clasificada como RESERVADA consistente en los Resultados de evaluación de riesgos de seguridad informática, de conformidad con lo establecido en el artículo 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública.

Versión pública, en la cual se testa información clasificada como RESERVADA consistente en los Resultados de evaluación de riesgos de seguridad informática, de conformidad con lo establecido en el artículo 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública.

#	Vulnerabilidad	Amenaza	Nivel de protección del sistema	Grado de exposición	Evaluación de probabilidad	Evaluación de impacto	Valor del riesgo	Nivel de riesgo

Versión pública, en la cual se testa información clasificada como RESERVADA consistente en los Resultados de evaluación de riesgos de seguridad informática, de conformidad con lo establecido en el artículo 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública.

#	Vulnerabilidad	Amenaza	Nivel de protección del sistema	Grado de exposición	Evaluación de probabilidad	Evaluación de impacto	Valor del riesgo	Nivel de riesgo

Versión pública, en la cual se testa información clasificada como RESERVADA consistente en los Resultados de evaluación de riesgos de seguridad informática, de conformidad con lo establecido en el artículo 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública.

Versión pública, en la cual se testa información clasificada como RESERVADA consistente en los Resultados de evaluación de riesgos de seguridad informática, de conformidad con lo establecido en el artículo 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública.

Versión pública, en la cual se testa información clasificada como RESERVADA consistente en los Resultados de evaluación de riesgos de seguridad informática, de conformidad con lo establecido en el artículo 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública.

Versión pública, en la cual se testa información clasificada como RESERVADA consistente en los Resultados de evaluación de riesgos de seguridad informática, de conformidad con lo establecido en el artículo 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública.

Establecimiento de los riesgos:

Versión pública, en la cual se testa información clasificada como RESERVADA consistente en los Resultados de evaluación de riesgos de seguridad informática, de conformidad con lo establecido en el artículo 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública.

Versión pública, en la cual se testa información clasificada como RESERVADA consistente en los Resultados de evaluación de riesgos de seguridad informática, de conformidad con lo establecido en el artículo 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública.

Versión pública, en la cual se testa información clasificada como RESERVADA consistente en los Resultados de evaluación de riesgos de seguridad informática, de conformidad con lo establecido en el artículo 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública.

#	Vulnerabilidad	Amenaza	Nivel de protección del sistema	Grado de exposición	Evaluación de probabilidad	Evaluación de impacto	Valor del riesgo	Nivel de riesgo

Versión pública, en la cual se testa información clasificada como RESERVADA consistente en los Resultados de evaluación de riesgos de seguridad informática, de conformidad con lo establecido en el artículo 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública.

#	Vulnerabilidad	Amenaza	Nivel de protección del sistema	Grado de exposición	Evaluación de probabilidad	Evaluación de impacto	Valor del riesgo	Nivel de riesgo

Versión pública, en la cual se testa información clasificada como RESERVADA consistente en los Resultados de evaluación de riesgos de seguridad informática, de conformidad con lo establecido en el artículo 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública.

Listado de riesgos:

Versión pública, en la cual se testa información clasificada como RESERVADA consistente en los Resultados de evaluación de riesgos de seguridad informática, de conformidad con lo establecido en el artículo 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública.

Versión pública, en la cual se testa información clasificada como RESERVADA consistente en los Resultados de evaluación de riesgos de seguridad informática, de conformidad con lo establecido en el artículo 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública.

Versión pública, en la cual se testa información clasificada como RESERVADA consistente en los Resultados de evaluación de riesgos de seguridad informática, de conformidad con lo establecido en el artículo 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública.

Versión pública, en la cual se testa información clasificada como RESERVADA consistente en los Resultados de evaluación de riesgos de seguridad informática, de conformidad con lo establecido en el artículo 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública.

Versión pública, en la cual se testa información clasificada como RESERVADA consistente en los Resultados de evaluación de riesgos de seguridad informática, de conformidad con lo establecido en el artículo 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública.

Versión pública, en la cual se testa información clasificada como RESERVADA consistente en los Resultados de evaluación de riesgos de seguridad informática, de conformidad con lo establecido en el artículo 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública.

#	Vulnerabilidad	Amenaza	Nivel de protección del sistema	Grado de exposición	Evaluación de probabilidad	Evaluación de impacto	Valor del riesgo	Nivel de riesgo

Versión pública, en la cual se testa información clasificada como RESERVADA consistente en los Resultados de evaluación de riesgos de seguridad informática, de conformidad con lo establecido en el artículo 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública.

#	Vulnerabilidad	Amenaza	Nivel de protección del sistema	Grado de exposición	Evaluación de probabilidad	Evaluación de impacto	Valor del riesgo	Nivel de riesgo

Versión pública, en la cual se testa información clasificada como RESERVADA consistente en los Resultados de evaluación de riesgos de seguridad informática, de conformidad con lo establecido en el artículo 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública.

Listado de riesgos:

Versión pública, en la cual se testa información clasificada como RESERVADA consistente en los Resultados de evaluación de riesgos de seguridad informática, de conformidad con lo establecido en el artículo 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública.

Versión pública, en la cual se testa información clasificada como RESERVADA consistente en los Resultados de evaluación de riesgos de seguridad informática, de conformidad con lo establecido en el artículo 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública.

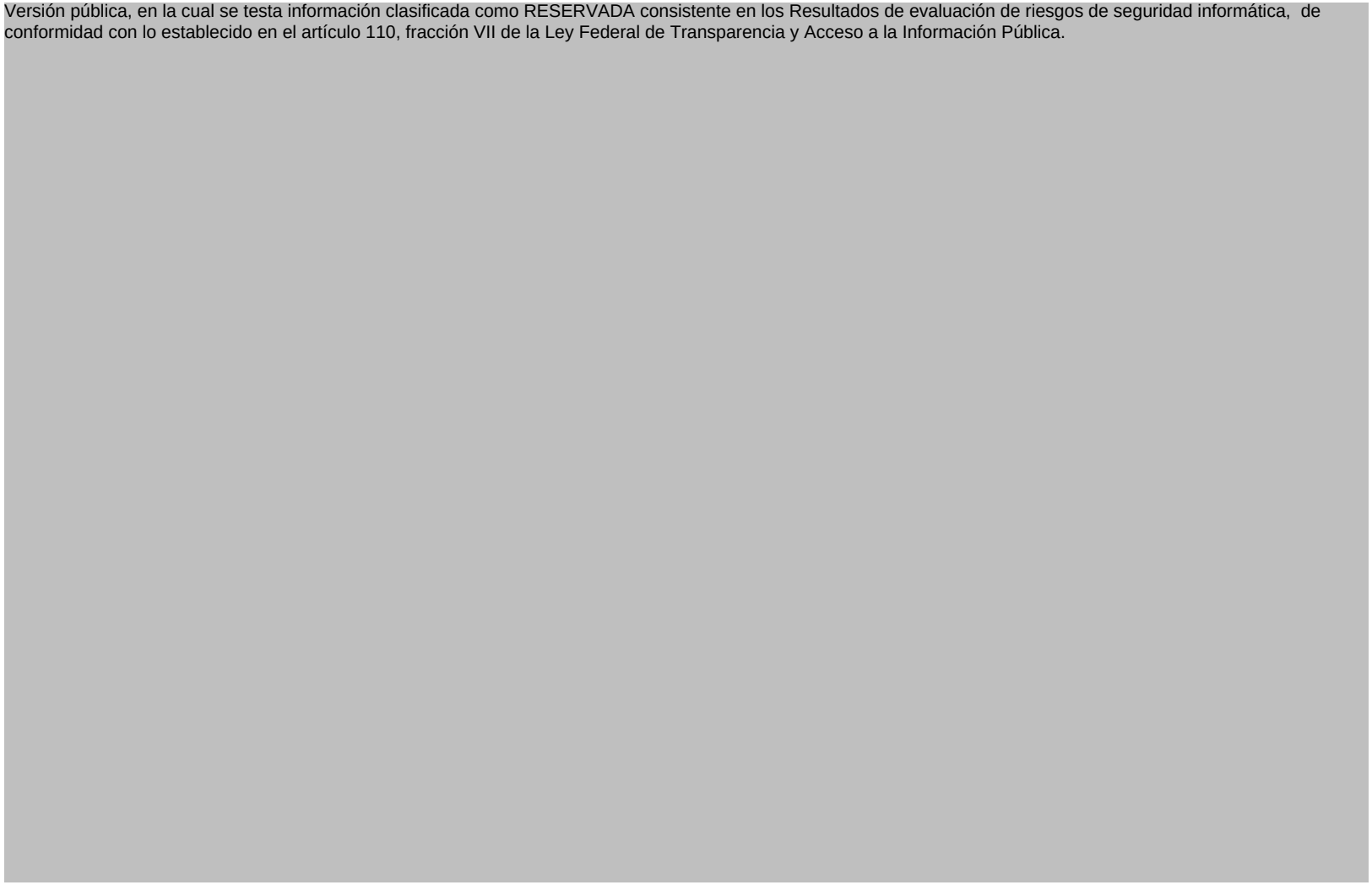
Versión pública, en la cual se testa información clasificada como RESERVADA consistente en los Resultados de evaluación de riesgos de seguridad informática, de conformidad con lo establecido en el artículo 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública.

Versión pública, en la cual se testa información clasificada como RESERVADA consistente en los Resultados de evaluación de riesgos de seguridad informática, de conformidad con lo establecido en el artículo 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública.

Versión pública, en la cual se testa información clasificada como RESERVADA consistente en los Resultados de evaluación de riesgos de seguridad informática, de conformidad con lo establecido en el artículo 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública.

- **Contramedidas en función de las vulnerabilidades identificadas**

Versión pública, en la cual se testa información clasificada como RESERVADA consistente en los Resultados de evaluación de riesgos de seguridad informática, de conformidad con lo establecido en el artículo 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública.



Versión pública, en la cual se testa información clasificada como RESERVADA consistente en los Resultados de evaluación de riesgos de seguridad informática, de conformidad con lo establecido en el artículo 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública.

Versión pública, en la cual se testa información clasificada como RESERVADA consistente en los Resultados de evaluación de riesgos de seguridad informática, de conformidad con lo establecido en el artículo 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública.

Versión pública, en la cual se testa información clasificada como RESERVADA consistente en los Resultados de evaluación de riesgos de seguridad informática, de conformidad con lo establecido en el artículo 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública.

Versión pública, en la cual se testa información clasificada como RESERVADA consistente en los Resultados de evaluación de riesgos de seguridad informática, de conformidad con lo establecido en el artículo 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública.

Versión pública, en la cual se testa información clasificada como RESERVADA consistente en los Resultados de evaluación de riesgos de seguridad informática, de conformidad con lo establecido en el artículo 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública.

Versión pública, en la cual se testa información clasificada como RESERVADA consistente en los Resultados de evaluación de riesgos de seguridad informática, de conformidad con lo establecido en el artículo 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública.

Versión pública, en la cual se testa información clasificada como RESERVADA consistente en los Resultados de evaluación de riesgos de seguridad informática, de conformidad con lo establecido en el artículo 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública.

Versión pública, en la cual se testa información clasificada como RESERVADA consistente en los Resultados de evaluación de riesgos de seguridad informática, de conformidad con lo establecido en el artículo 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública.

Versión pública, en la cual se testa información clasificada como RESERVADA consistente en los Resultados de evaluación de riesgos de seguridad informática, de conformidad con lo establecido en el artículo 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública.

Versión pública, en la cual se testa información clasificada como RESERVADA consistente en los Resultados de evaluación de riesgos de seguridad informática, de conformidad con lo establecido en el artículo 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública.

Versión pública, en la cual se testa información clasificada como RESERVADA consistente en los Resultados de evaluación de riesgos de seguridad informática, de conformidad con lo establecido en el artículo 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública.

Versión pública, en la cual se testa información clasificada como RESERVADA consistente en los Resultados de evaluación de riesgos de seguridad informática, de conformidad con lo establecido en el artículo 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública.

11. Control Documental

Versión	Fecha	Clasificación	Autor del cambio	Descripción del cambio
v1.0	17-oct-2019	Reservada	Dirección de Seguridad Informática	Documento original publicado
V2.0	28-feb-2023	Reservada	Dirección de Seguridad Informática	Actualización
V2.1	30-jun-2023	Reservada	Dirección de Seguridad Informática	Actualización de FODA, clasificación de la información y homologación de criterios para documentación, Roles y responsabilidades en función de los grupos de trabajo, Plan de comunicación y descripción de procedimientos.

12. Aprobación del documento

Rol	Nombre y Cargo
Aprobó:	**Mtro. Omar Salinas** Director de Seguridad Informática
Revisó:	**Mtro. José Eduardo Girón Camacho** Subdirector de Ciberseguridad
Revisó:	**Mtro. Ramón Caballero Ledesma** Subdirector de Cumplimiento de Seguridad Informática
Elaboró	**Ing. Erika Hernández Fernández** Jefa de Departamento de Controles de Seguridad Informática

El presente documento se firma digitalmente de conformidad a lo establecido en el artículo 3 del Acuerdo General de Administración III/2020, del presidente de la Suprema Corte de Justicia de la Nación, del 17 de septiembre de 2020, por el que se regula el trámite electrónico y uso de la firma electrónica certificada del Poder Judicial de la Federación (FIREL) para actuaciones administrativas.