

**Manual del sistema de gestión de seguridad de la información, ciberseguridad y protección de datos personales**

**SIGCMA**

VERSIÓN 02

SEPTIEMBRE 2022

**Control de versiones**

|  |  |  |  |
| --- | --- | --- | --- |
| Versión | Fecha | Comentarios | Por |
| 1 | 28-07-2022 | Versión Inicial | GPET |
| 2 | 29-09-2022 | Modificación a la política del SGSI, objetivos y alcance | SIGCMA / UI / GPET |
|  |  |  |  |

**Historial de revisiones**

|  |  |  |  |
| --- | --- | --- | --- |
| Revisión | Fecha | Comentarios | Por |
| 0.1 | 25-02-2022 | Versión Inicial | GPET |
| 0.2 | 17-03-2022 | Ajustes de acuerdo con información levantada en entrevistas con la Rama Judicial. | GPET |
| 0.3 | 11-04-2022 | Ajuste según presentación al Equipo de Proyectos Especiales. | GPET |
| 1.0 | 19-04-2022 | Versión para revisión por el CSJ | GPET |
| 1.1 | 28-04-2022 | Ajustes de acuerdo con las observaciones del 26-04-2022. | GPET |
| 1.2 | 29-04-2022 | Ajustes de acuerdo a reunión interna del 29-04-2022. | GPET |
| 2.0 | 02-05-2022 | Versión para revisión por el CSJ | GPET |
| 3.0 | 03-07-2022 | Ajustes de acuerdo con observaciones del Grupo de Proyectos Especiales de Tecnología. | GPET |
| 4.0 | 31-08-2022 | Modificación a la política del SGSI, objetivos y alcance | GPET |

**TABLA DE CONTENIDO**

[1. INTRODUCCIÓN 6](#_Toc116649908)

[2. OBJETIVO 6](#_Toc116649909)

[2.1. General 6](#_Toc116649910)

[2.2. Específicos 6](#_Toc116649911)

[3. TÉRMINOS Y DEFINICIONES 7](#_Toc116649912)

[4. CONTEXTO ORGANIZACIONAL 7](#_Toc116649913)

[4.1. Conocimiento de la Organización y de su Contexto 7](#_Toc116649914)

[4.1.1. Corporaciones que conforman la Rama Judicial 7](#_Toc116649915)

[4.1.2. Análisis del Contexto Organizacional 11](#_Toc116649916)

[4.1.3. Contexto Externo 11](#_Toc116649917)

[4.1.4. Contexto Interno 11](#_Toc116649918)

[4.2. Comprensión de las Necesidades y Expectativas de las Partes Interesadas. 12](#_Toc116649919)

[4.3. Alcance de Implementación del Sistema de Gestión de Seguridad de la Información, Ciberseguridad y Protección de Datos Personales 13](#_Toc116649920)

[4.4. Alcance de Certificación año 2022 15](#_Toc116649921)

[5. LIDERAZGO Y COMPROMISO 15](#_Toc116649922)

[5.1. Política del Sistema de Gestión de Seguridad de la Información, Ciberseguridad y Protección de Datos Personales para la Rama Judicial 15](#_Toc116649923)

[5.2. Roles y Responsabilidades del Sistema de Gestión de Seguridad de la Información, Ciberseguridad y Protección de Datos Personales para la Rama Judicial 15](#_Toc116649924)

[5.2.1. Normograma 17](#_Toc116649925)

[5.2.2. Comité de Seguridad de la Información 19](#_Toc116649926)

[5.2.3. Oficina de Seguridad de la Información 20](#_Toc116649927)

[5.2.1. Director de la Oficina de Seguridad de la Información 22](#_Toc116649928)

[5.2.2. Oficial de Seguridad de la Información 23](#_Toc116649929)

[5.2.3. Coordinador de Protección de Datos Personales 23](#_Toc116649930)

[5.2.4. Coordinador de Ciberseguridad 24](#_Toc116649931)

[5.2.5. Coordinador de Seguridad de la Información 24](#_Toc116649932)

[5.2.6. Analistas de Ciberseguridad 25](#_Toc116649933)

[5.2.7. Analistas de Seguridad de la Información 25](#_Toc116649934)

[5.2.8. Líderes de proceso 25](#_Toc116649935)

[5.2.9. Servidores Judiciales 26](#_Toc116649936)

[5.2.10. Auditoría Interna o Externa 26](#_Toc116649937)

[6. PLANIFICACIÓN 26](#_Toc116649938)

[6.1. Acciones para tratar riesgos y oportunidades 26](#_Toc116649939)

[6.1.1. Generalidades 26](#_Toc116649940)

[6.1.2. Identificación y Valoración de Riesgos de Seguridad de la Información 28](#_Toc116649941)

[6.1.3. Tratamiento de Riesgos de seguridad de la información 29](#_Toc116649942)

[6.2. Objetivos del Sistema de Gestión de Seguridad de la Información, Ciberseguridad y Protección de Datos Personales para la Rama Judicial 29](#_Toc116649943)

[6.2.1. Seguridad de la Información: 29](#_Toc116649944)

[7. SOPORTE 30](#_Toc116649945)

[7.1. Recursos 30](#_Toc116649946)

[7.2. Competencia 31](#_Toc116649947)

[7.3. Toma de Conciencia 31](#_Toc116649948)

[7.4. Comunicación 31](#_Toc116649949)

[7.5. Control Documental 32](#_Toc116649950)

[8. OPERACIÓN 33](#_Toc116649951)

[8.1. Planificación y Control Operacional 33](#_Toc116649952)

[8.2. Valoración de Riesgos 34](#_Toc116649953)

[8.3. Plan de Tratamiento de los Riesgos 35](#_Toc116649954)

[9. EVALUACIÓN DEL DESEMPEÑO 35](#_Toc116649955)

[9.1. Seguimiento, Medición, Análisis y Evaluación 35](#_Toc116649956)

[9.2. Auditoria al SGSI 36](#_Toc116649957)

[9.2.1. Auditoría Interna 36](#_Toc116649958)

[9.2.2. Auditoría Externa 37](#_Toc116649959)

[9.3. Revisión por la Dirección 37](#_Toc116649960)

[10. MEJORA 37](#_Toc116649961)

[10.1. No conformidades y Acción Correctiva 38](#_Toc116649962)

[10.1.1. Identificación de las no Conformidades 38](#_Toc116649963)

[10.1.2. Acciones Correctivas 38](#_Toc116649964)

[10.1.3. Prevención de las No Conformidades 39](#_Toc116649965)

[10.1.4. Registro de las No Conformidades 39](#_Toc116649966)

[10.1.5. Resultados de las Acciones Correctivas y Preventivas 39](#_Toc116649967)

[10.2. Mejora Continua 39](#_Toc116649968)

[11. ANEXOS 41](#_Toc116649969)

[11.1. Anexo A. Plan de Gestión de los Interesados 41](#_Toc116649970)

[11.2. Anexo B. Análisis FODA 49](#_Toc116649971)

[11.2.1. Estrategias Fortalezas - Oportunidades 49](#_Toc116649972)

[11.2.2. Estrategias Fortalezas - Amenazas 50](#_Toc116649973)

[11.2.3. Estrategias Debilidades - Amenazas 51](#_Toc116649974)

[11.2.4. Estrategias Debilidades - Oportunidades 52](#_Toc116649975)

[11.2.5. Resultados análisis FODA 53](#_Toc116649976)

[11.3. Anexo C. Plan de mejoramiento 55](#_Toc116649977)

[11.4. Anexo D. Perfiles del SGSI 56](#_Toc116649978)

**ÍNDICE DE TABLAS**

[Tabla 1. Estrategias Partes Interesadas 13](#_Toc116649979)

[Tabla 2. Nivel – Compromiso Partes Interesadas 13](#_Toc116649980)

[Tabla 3. Aplicación de indicadores en las corporaciones de la Rama Judicial 36](#_Toc116649981)

**ÍNDICE DE ILUSTRACIONES**

[Ilustración 1. Estructura organizacional CSJ 7](#_Toc116649992)

[Ilustración 2. Estructura organizacional Corte Suprema de Justicia 8](#_Toc116649993)

[Ilustración 3. Estructura organizacional Consejo de Estado 9](#_Toc116649994)

[Ilustración 4. Estructura organizacional Corte Constitucional 10](#_Toc116649995)

[Ilustración 5. Matriz Poder / Interés 12](#_Toc116649996)

[Ilustración 6. Alcance a nivel de procesos CSJ 14](#_Toc116649997)

[Ilustración 7. Ubicación de la Oficina de Seguridad de la Información 21](#_Toc116649998)

[Ilustración 8. Estructura de la Oficina de Seguridad de la Información 22](#_Toc116649999)

[Ilustración 9. Matriz FODA 27](#_Toc116650000)

[Ilustración 10. Metodología de gestión de riesgos integrada 28](#_Toc116650001)

1. INTRODUCCIÓN

Este manual contiene los aspectos claves para la definición, implementación, operación, monitoreo y mejora continua del Sistema de Gestión de Seguridad de la Información, Ciberseguridad y Protección de Datos Personales, según las mejores prácticas establecidas en la norma ISO 27001:2013, ISO 27032:2012, así como dar cumplimiento a la Ley 1581 de 2012 (la cual establece disposiciones generales para la protección de datos personales), Ley 1712 de 2014 (Regula el derecho de acceso a la información pública) y a lo establecido en la Política de Gobierno Digital de MINTIC para la implementación del Modelo de Seguridad y Protección de Datos Personales (MSPI).

1. OBJETIVO
   1. General

Diseñar, establecer, implementar, operar y mantener un Sistema de Gestión de Seguridad de la Información, Ciberseguridad y Protección de Datos Personales, según lo establecido en las normas ISO 27001:2013, ISO 27032:2012, así como en la Ley 1581 de 2012 de Protección de Datos Personales y la Ley 1712 de 2014 de Transparencia y en el Modelo de Seguridad y Privacidad de la Información de MINTIC, con el fin de asegurar la confidencialidad, disponibilidad e integridad de la información de la Rama Judicial.

* 1. Específicos
* Establecer el contexto organizacional para el Sistema de Gestión de Seguridad de la Información, Ciberseguridad y Protección de Datos Personales para la Rama Judicial.
* Definir el alcance del Sistema de Gestión de Seguridad de la Información, Ciberseguridad y Protección de Datos Personales para la Rama Judicial.
* Identificar los interesados en el Sistema de Gestión de Seguridad de la Información, Ciberseguridad y Protección de Datos Personales para la Rama Judicial.
* Establecer las directrices de la política del Sistema de Gestión de Seguridad de la Información, Ciberseguridad y Protección de Datos Personales para la Rama Judicial.
* Definir roles y responsabilidades para el Sistema de Gestión de Seguridad de la Información, Ciberseguridad y Protección de Datos Personales para la Rama Judicial del Equipo de Trabajo, con el fin de garantizar el cumplimiento de los objetivos planteados para el sistema.
* Definir las directrices para la gestión de riesgos de seguridad de la información.
* Establecer los recursos necesarios para el óptimo funcionamiento del Sistema de Gestión de Seguridad de la Información, Ciberseguridad y Protección de Datos Personales para la Rama Judicial.
* Definir los indicadores del Sistema de Gestión de Seguridad de la Información, Ciberseguridad y Protección de Datos Personales para la Rama Judicial.

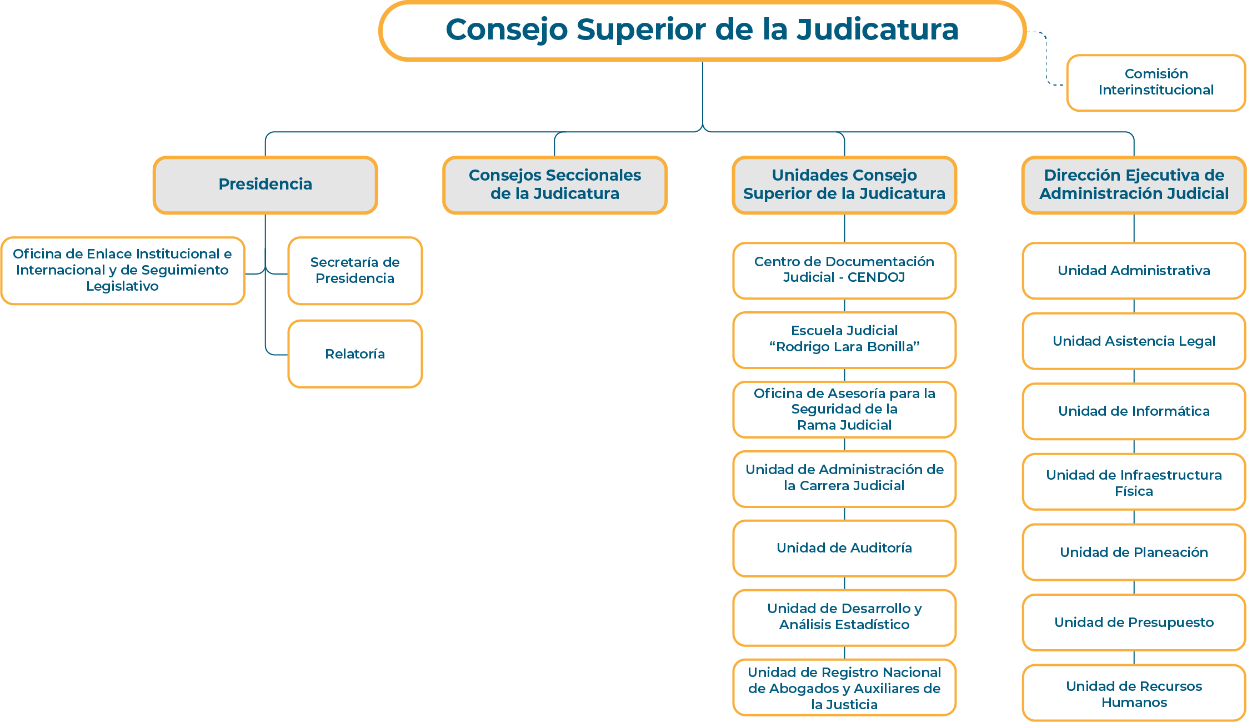
1. TÉRMINOS Y DEFINICIONES

El glosario del Sistema de Gestión de Seguridad de la Información, Ciberseguridad y Protección de Datos Personales para la Rama Judicial se encuentra unificado en el documento [GLOSARIO del SGSI.](https://etbcsj.sharepoint.com/teams/GrupoCertificacin27001DEAJ/Documentos%20compartidos/General/Estructura%20ISO%2027001%20V2/2.%20Planear%20-%20Numerales%204,%205,%206%20y%207/GLOSARIO%20SGSI%20V1.docx) Por favor consultar dicho documento.

1. CONTEXTO ORGANIZACIONAL
   1. Conocimiento de la Organización y de su Contexto
      1. Corporaciones que conforman la Rama Judicial

**Consejo Superior de la Judicatura**

El Consejo Superior de la Judicatura con origen en la misma judicatura, se encarga del gobierno y la administración integral de la Rama Judicial , en aspectos tales como la reglamentación de la ley, la planeación, programación y ejecución del presupuesto, la administración del talento humano a través de la carrera judicial, la elaboración de listas de candidatos a los cargos de magistrado de la Corte Suprema de Justicia y del Consejo de Estado, adelantar programas de formación y capacitación para los servidores de la Rama Judicial, controlar el rendimiento de los despachos judiciales, fijar la división del territorio para efectos judiciales, ubicar, redistribuir y fusionar despachos judiciales, crear, suprimir, fusionar y trasladar cargos, suministrar sedes y elementos a los despachos judiciales, llevar el control de desempeño de los funcionarios y empleados para garantizar el ejercicio legal de la profesión de abogado. En la ilustración 1 se muestra la estructura organizacional del Consejo Superior del Judicatura (CSJ):

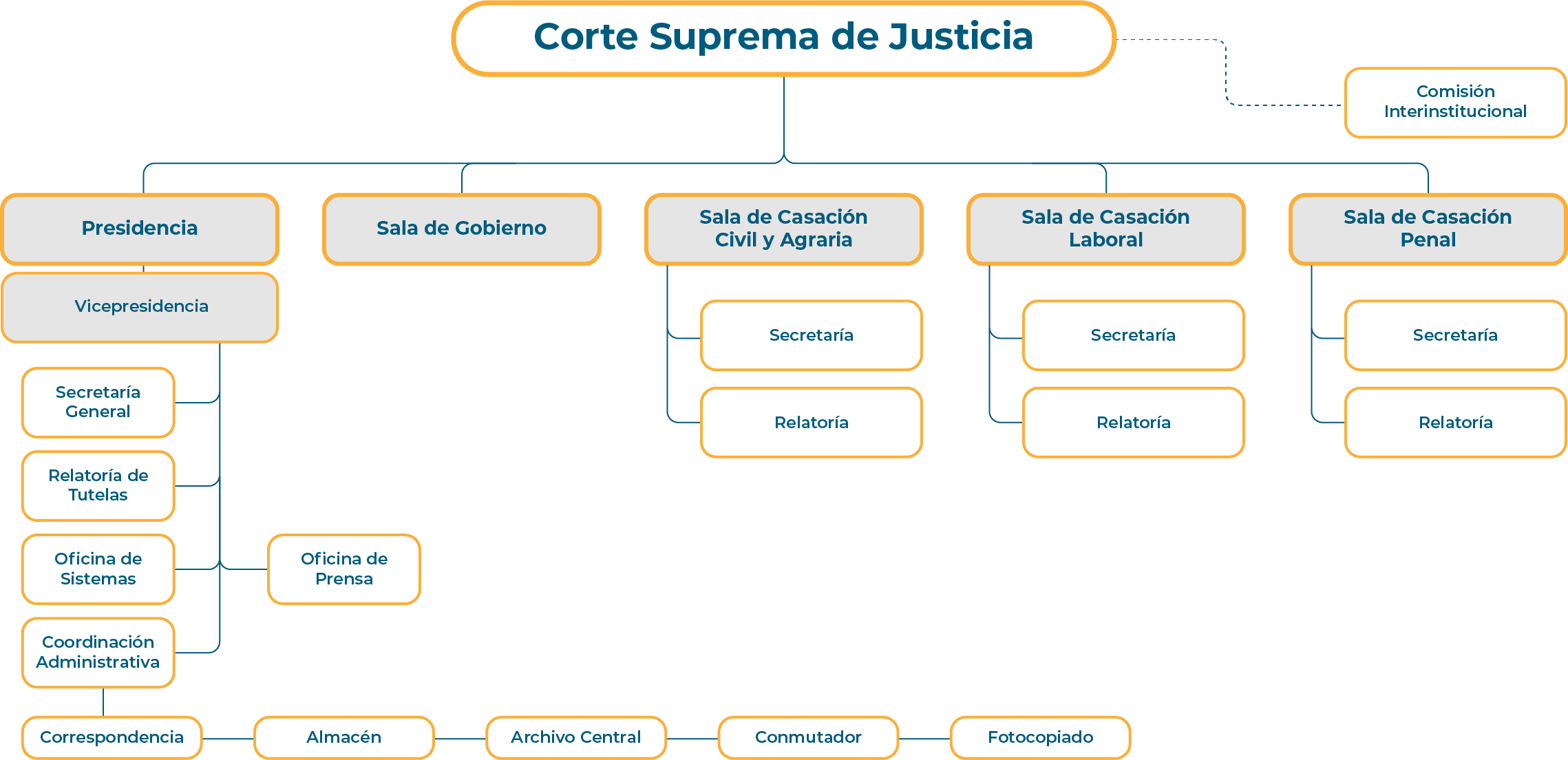


**Ilustración 1. Estructura organizacional CSJ**

**Corte Suprema de Justicia**

La Corte Suprema de Justicia es el máximo tribunal de la jurisdicción ordinaria y se compone del número impar de magistrados que determine la ley. Esta divide la Corte en Salas, señalará a cada una de ellas los asuntos que deba conocer separadamente y determinará aquellos en que deba intervenir la Corte en pleno. Son atribuciones de la Corte Suprema de Justicia, entre otras:

1. Actuar como tribunal de casación.
2. Juzgar al Presidente de la República o a quien haga sus veces y a los altos funcionarios de que trata el artículo 174, por cualquier hecho punible que les impute, conforme al artículo 175 numerales 2 y 3.
3. Investigar y juzgar a los miembros del Congreso.
4. Juzgar, previa acusación del Fiscal General de la Nación, del Vicefiscal General de la Nación o de sus delegados de la Unidad de Fiscalías ante la Corte Suprema de Justicia, a los Ministros del Despacho, al Procurador General de la Nación, al Defensor del Pueblo, a los agentes del Ministerio Público ante la Corte, ante el Consejo de Estado y ante los tribunales; a los directores de los Departamentos Administrativos, al Contralor General de la República, a los Embajadores y jefes de misión diplomática o consular, a los Gobernadores, a los Magistrados de Tribunales y a los Generales y Almirantes de la Fuerza Pública, por los hechos punibles que se les imputen.
5. Conocer de todos los negocios contenciosos de los agentes diplomáticos acreditados ante el Gobierno de la Nación, en los casos previstos por el Derecho Internacional.
6. Darse su propio reglamento.
7. Las demás atribuciones que señale la ley.



**Ilustración 2. Estructura organizacional Corte Suprema de Justicia**

**Consejo de Estado**

El Consejo de Estado es el tribunal supremo de la jurisdicción de lo contencioso administrativo, y en tal virtud conoce de las acciones de nulidad por inconstitucionalidad contra los decretos dictados por el Gobierno Nacional que no sean de competencia de la Corte Constitucional, de los casos de pérdida de investidura de los congresistas y de la acción de nulidad electoral de acuerdo a la ley, resuelve las controversias y litigios de mayor importancia originados en actos, contratos, hechos, omisiones y operaciones sujetos al derecho administrativo, en los que estén involucradas las entidades públicas o los particulares cuando ejerzan función administrativa. Así mismo fija las pautas jurisprudenciales que las autoridades, magistrados y jueces de la jurisdicción deben atender para resolver casos similares.

También actúa como cuerpo supremo consultivo del Gobierno Nacional en asuntos de administración a través de la Sala de Consulta y Servicio Civil, encargada de absolver las consultas formuladas por los ministros y los directores de departamentos administrativos. También resuelve los conflictos de competencias administrativas y está facultada para presentar ante el Congreso de la República proyectos de ley y de reforma a la Constitución Política.

En la ilustración 3 se presenta la estructura organizacional del Consejo de Estado:



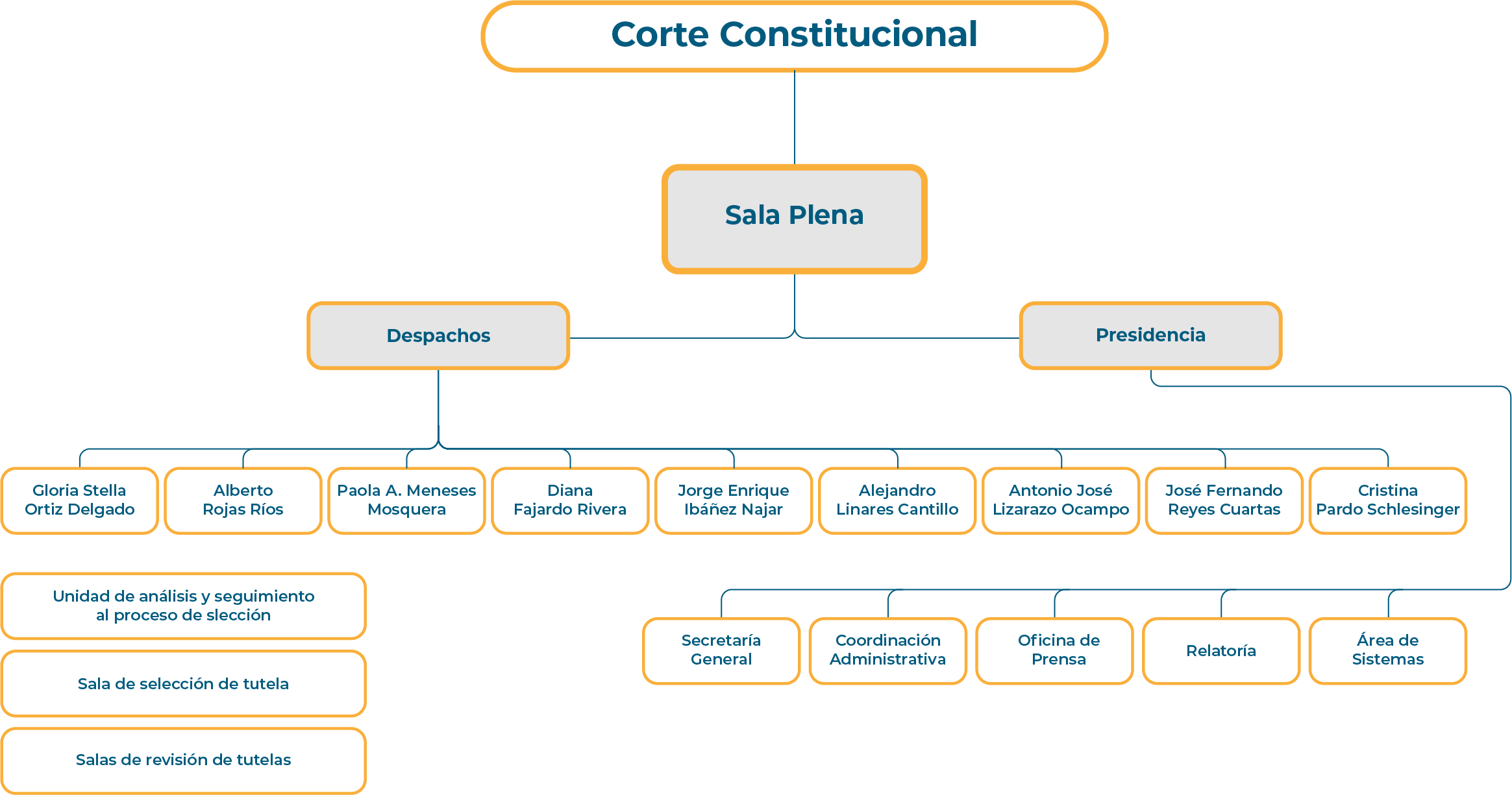
**Ilustración 3. Estructura organizacional Consejo de Estado**

**Corte Constitucional**

La Corte Constitucional es una institución de la Rama Judicial del Poder Público creada mediante la adopción de la Constitución de 1991 con el fin de guardar la integridad y supremacía de la Carta Política. La Corte está integrada por nueve magistrados, nombrados por el Senado de la República para períodos individuales de ocho años de ternas enviadas por el Presidente de la República, la Corte Suprema de Justicia y el Consejo de Estado. De acuerdo con el artículo 241 de la Constitución Política, son funciones de la Corte Constitucional, entre otras:

1. Decidir sobre las demandas de inconstitucionalidad que promuevan los ciudadanos contra los actos reformatorios de la Constitución, cualquiera que sea su origen, sólo por vicios de procedimiento en su formación.
2. Decidir, con anterioridad al pronunciamiento popular, sobre la constitucionalidad de la convocatoria a un referendo o a una Asamblea Constituyente para reformar la Constitución, sólo por vicios de procedimiento en su formación.
3. Decidir sobre la constitucionalidad de los referendos sobre leyes y de las consultas populares y plebiscitos del orden nacional. Estos últimos sólo por vicios de procedimiento en su convocatoria y realización.
4. Decidir sobre las demandas de inconstitucionalidad que presenten los ciudadanos contra las leyes, tanto por su contenido material como por vicios de procedimiento en su formación.
5. Revisar, en la forma que determine la ley, las decisiones judiciales relacionadas con la acción de tutela de los derechos constitucionales.
6. Decidir definitivamente sobre la exequibilidad de los tratados internacionales y de las leyes que los aprueben.

La ilustración 4 presenta la estructura organizacional de la Corte Constitucional:



**Ilustración 4. Estructura organizacional Corte Constitucional**

**Comisión Nacional de Disciplina Judicial**

La Comisión Nacional de Disciplina Judicial fue instituida por la Constitución con el fin de garantizar la existencia, al interior de la propia Rama Judicial, de un organismo autónomo, imparcial e independiente de alto rango con funciones de naturaleza jurisdiccional, que tuviera a su cargo la tarea de administrar justicia en materia disciplinaria sobre los funcionarios y empleados judiciales y los abogados.

La Constitución de 1991 creó esta jurisdicción al mismo nivel jerárquico de la ordinaria, constitucional y contencioso administrativo; sus decisiones en materia disciplinaria son verdaderas sentencias, no sujetas a posterior estudio y pronunciamiento de otra jurisdicción, salvo que se accione en tutela por haber incurrido en una vía de hecho.

Hacen parte de esta jurisdicción las siguientes dependencias:

* Secretaría Judicial
* Comisiones Seccionales de Disciplina Judicial
* Sistemas
* Relatoría
* Comunicaciones
  + 1. Análisis del Contexto Organizacional

A continuación, se presenta la metodología para el análisis del contexto organizacional, tomando como base lo establecido en la Norma Técnica Colombiana NTC ISO 31000, para mayor detalle ver el documento “[Contexto Organizacional SGSI](https://etbcsj.sharepoint.com/teams/GrupoCertificacin27001DEAJ/Documentos%20compartidos/General/Estructura%20ISO%2027001%20V2/2.%20Planear%20-%20Numerales%204,%205,%206%20y%207/Contexto%20Organizacional%20SGSI%20%20V1.docx)” el cual detalla el contexto externo e interno de la Rama Judicial, en el cual se enmarca el alcance de este sistema.

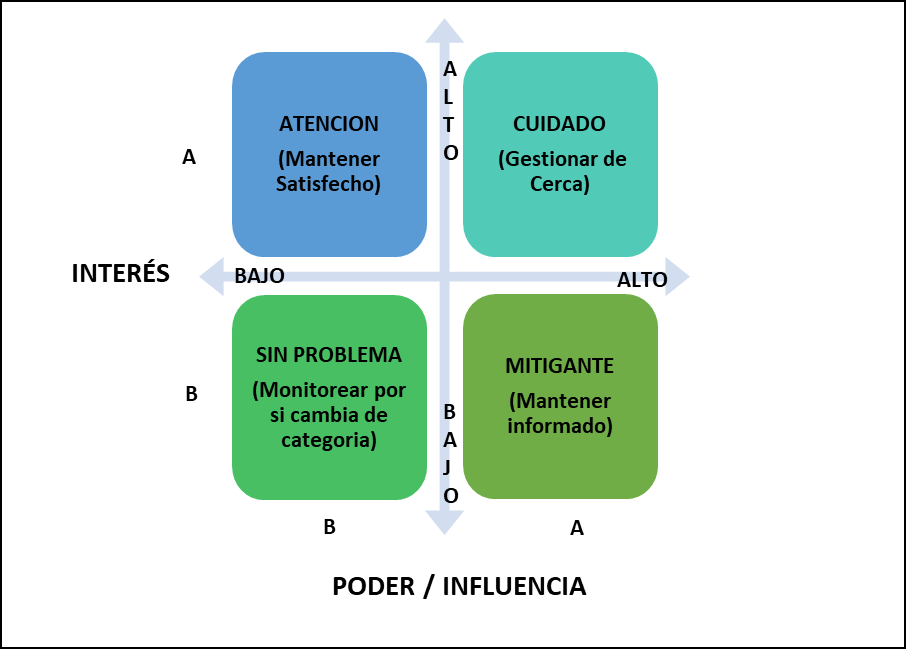
* + 1. Contexto Externo
* Social
* Cultural
* Político
* Legal
* Reglamentario
* Financiero
* Tecnológico
* Económico
* Ambiental
  + 1. Contexto Interno
* Visión, misión y valores
* Gobernanza, estructura organizacional
* Estrategia, objetivos y políticas
* Cultura organizacional
* Normas, directrices, modelos adoptados
* Recursos (capital, tiempo, personas, procesos, sistemas de información)
* Relaciones con partes interesadas internas
* Relaciones contractuales

Por otra parte, la normatividad asociada al Sistema de Gestión de Seguridad de la Información, Ciberseguridad y protección de Datos Personales en la Rama Judicial se puede observar en detalle en el documento “[Normograma SGSI CSJ](https://etbcsj.sharepoint.com/teams/Proyecto166-2021SGSI/Documentos%20compartidos/General/SGSI/02%20-%20Etapa%20de%20Ejecución/06%20-%20DOCUMENTOS%20REVISIÓN/Estructura%20ISO%2027001%20V2/2.%20Planear%20-%20Numerales%204,%205,%206%20y%207/Normas%20SGSI%20CSJ%20V1.xlsx)”.

* 1. Comprensión de las Necesidades y Expectativas de las Partes Interesadas.

A continuación, se presenta la metodología para el análisis de las partes interesadas en el Sistema de Gestión de Seguridad de la Información, Ciberseguridad y Protección de Datos Personales para la Rama Judicial, mediante el cual se identifican personas, entidades u organizaciones que puedan ser afectados por el sistema, así mismo todos los que por su poder también puedan influir de alguna forma en la implementación del sistema.

Las partes interesadas se clasifican con base en su nivel poder / influencia y su interés en el diseño, planeación, implementación, operación y mejora continua del SGSI, tal como se presenta en la ilustración 5:



**Ilustración 5. Matriz Poder / Interés[[1]](#footnote-2)**

A continuación, se desarrollan diferentes estrategias para gestionar a los interesados en el SGSI:

| **Poder / Influencia** | **Interés** | **Estrategia** | **Descripción de la Estrategia** |
| --- | --- | --- | --- |
| A | A | Gestionar de cerca | Entregar la información del Sistema de Gestión de Seguridad de la Información, Ciberseguridad y Protección de Datos Personales tan pronto como sea posible, utilizando medios de comunicación rápidos y efectivos (llamadas telefónicas, videoconferencias, reuniones presenciales).  Realizar reuniones de seguimiento semanales para informar los avances y contratiempos del sistema. |
| A | B | Mantener satisfecho | Entregar información oportunamente para que puedan ejercer sus funciones según los tiempos establecidos en el SGSI.  Realizar campañas de concienciación sobre el sistema, para aumentar el interés por parte de los interesados. |
| B | A | Mantener Informado | Resolver sus necesidades de información dentro de los tiempos establecidos. |
| B | B | Monitorear por si cambia de categoría | Evaluar el comportamiento, para verificar si el compromiso cambia dando lugar a un cambio en el nivel de poder - influencia e interés. |

**Tabla 1. Estrategias Partes Interesadas**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **NIVEL  PODER / INTERÉS** | |  | **COMPROMISO** | |
| A | Alto |  | X | Actual |
| B | Bajo |  | D | Deseado |

**Tabla 2. Nivel – Compromiso Partes Interesadas**

En el Anexo A. [Plan de Gestión de los Interesados,](https://etbcsj.sharepoint.com/teams/GrupoCertificacin27001DEAJ/Documentos%20compartidos/General/Estructura%20ISO%2027001%20V2/2.%20Planear%20-%20Numerales%204,%205,%206%20y%207/Anexo%20A.%20Plan%20de%20Gestión%20de%20los%20Interesados%20V1.xlsx) se presenta la identificación y valoración de las partes interesadas para la implementación del Sistema de Gestión de Seguridad de la Información, Ciberseguridad y Protección de Datos Personales de la Rama Judicial, incluyendo el planteamiento de estrategias para los mismos según su clasificación.

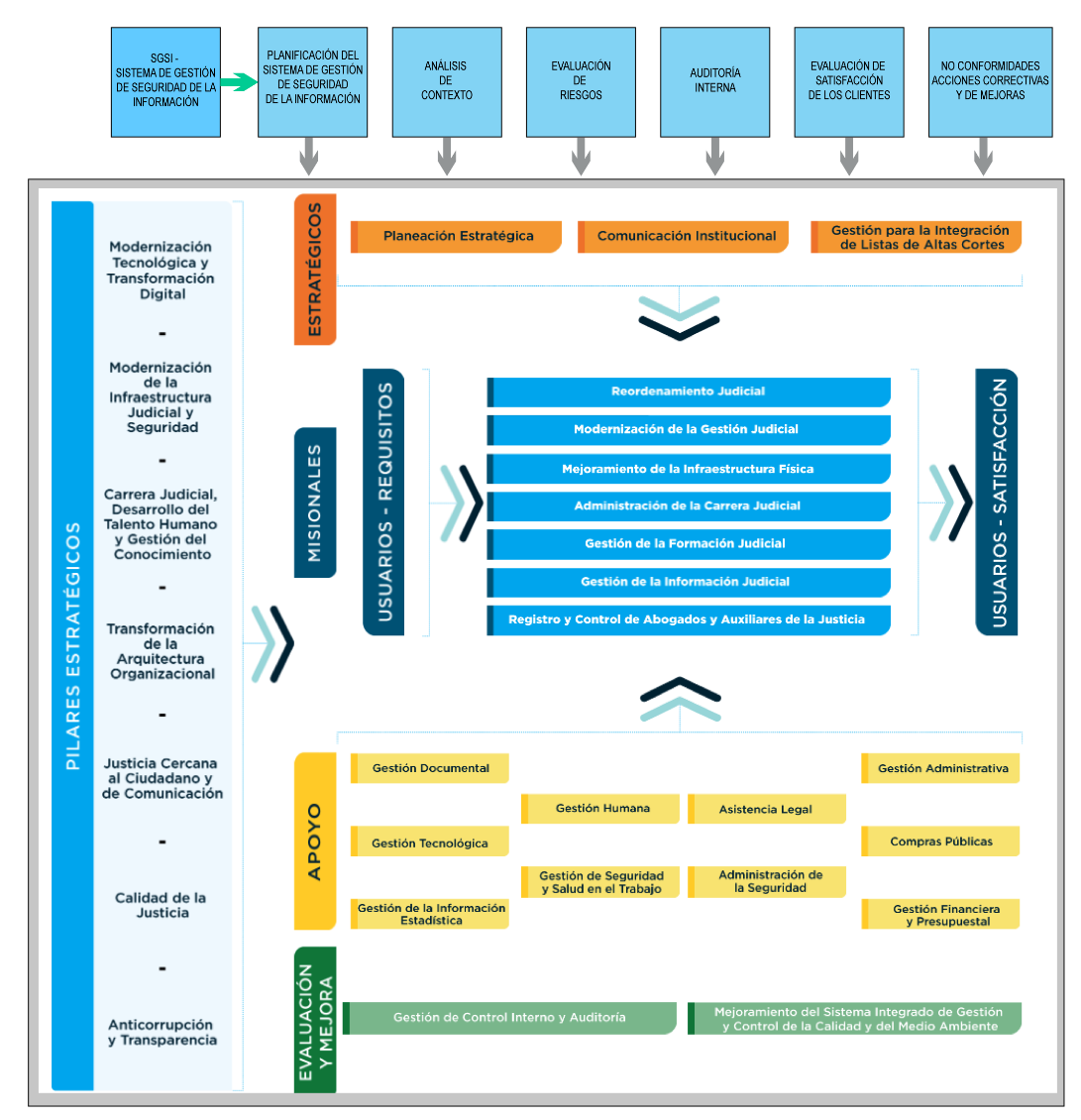
* 1. Alcance de Implementación del Sistema de Gestión de Seguridad de la Información, Ciberseguridad y Protección de Datos Personales

El Sistema de Gestión de Seguridad de la Información, Ciberseguridad y Protección de Datos Personales abarca los activos y contenedores de información gestionados por todos los procesos estratégicos, misionales, de apoyo, y de evaluación y mejora del Consejo Superior de la Judicatura (CSJ) y de la Dirección Ejecutiva de Administración Judicial (DEAJ), con el fin de garantizar su confidencialidad, integridad y disponibilidad de la información.

Las corporaciones incluidas en el alcance del SGSI son:

* Consejo Superior de la Judicatura.
* Dirección Ejecutiva de Administración Judicial

El SGSI cubre todas las actividades de los procesos del Consejo Superior de la Judicatura.



**Ilustración 6. Alcance a nivel de procesos CSJ**

El Consejo Superior de la Judicatura, depende de los siguientes proveedores externos de servicios tecnológicos, importantes para la gestión eficaz de la cadena de valor:

* Oficina de Seguridad de la Información – SOC
* Servicio de telecomunicaciones
* Servicio de Datacenter en nube
* Servicio de Datacenter en Colocation
* Licenciamiento de software

Además, es importante mencionar que el CSJ realiza interoperabilidades con entidades gubernamentales, garantizando la seguridad de la información expuesta y consumida, cumpliendo con los lineamientos del aliado estratégico Ministerio de las Tecnologías de la Información y las Comunicaciones.

No se tienen exclusiones en la implementación del Sistema de Gestión de Seguridad de la Información, Ciberseguridad y Protección de Datos Personales según lo establecido en las normas ISO 27001:2013, ISO 27032, la ley 1581 de 2012 y el Modelo de Seguridad y Privacidad de la Información de MINTIC.

* 1. Alcance de Certificación año 2022

Para la vigencia 2022 de acuerdo por los lineamientos establecidos por la Magistrada líder del SIGCMA en su Calidad de representante de la Alta Dirección, se presentará a procesos de certificación la Unidad de Informática y el Grupo de Proyectos Especiales en Tecnología de la Dirección Ejecutiva de Administración Judicial – DEAJ.

Ubicación: Palacio de Justicia y DEAJ

1. LIDERAZGO Y COMPROMISO
   1. Política del Sistema de Gestión de Seguridad de la Información, Ciberseguridad y Protección de Datos Personales para la Rama Judicial

En cumplimiento de su función constitucional de hacer efectivos los derechos, obligaciones, garantías y libertades para lograr la convivencia social, la convivencia pacífica y el acceso a la justicia, el Consejo Superior de la Judicatura se compromete a la protección de los activos de información, manteniendo un nivel de exposición al riesgo que permita responder por la integridad, confidencialidad, autenticidad y disponibilidad de la información.

El Consejo Superior de la Judicatura a través de esta política reafirma su compromiso con el cumplimiento de los requisitos legales y demás aplicables a todo su sistema de gestión y con la definición, implementación de controles efectivos que le permitan el cumplimiento de su misión institucional y el mejoramiento continuo del sistema integrado de gestión SIGCMA.

* 1. Roles y Responsabilidades del Sistema de Gestión de Seguridad de la Información, Ciberseguridad y Protección de Datos Personales para la Rama Judicial

Actualmente el Grupo de Proyectos Especiales de Tecnología GPET tiene las siguientes funciones asignadas mediante el ACUERDO PCSJA20-11603 del 27/07/2020 y PCSJA20-11700 23/12/2020, relacionadas con la gestión de seguridad de la información en la Rama Judicial:

1. Apoyar, al Consejo Superior de la Judicatura y al director ejecutivo de Administración Judicial, en la definición de propuestas de políticas, estándares y lineamientos de seguridad de la información y ciberseguridad de la Rama Judicial, de conformidad con la normativa, estándares y mejores prácticas.
2. Proponer a la instancia correspondiente proyectos para la implementación, mantenimiento y mejora continua del Modelo de Seguridad y Privacidad de la Información - MSPI, con base en las mejores prácticas y siguiendo los lineamientos del Ministerio de las Tecnologías de la Información y las Comunicaciones o quien haga sus veces.
3. Apoyar y proponer lineamientos para la configuración de las herramientas de seguridad informática para la gestión de vulnerabilidades, riegos e incidentes de seguridad.
4. Verificar el cumplimiento de indicadores y métricas de seguridad de la información, tanto a nivel técnico como a nivel estratégico, solicitar a la instancia técnica correspondiente la elaboración de los planes de mejora y monitorear su cumplimiento.

Por otra parte, las funciones de la Unidad de Informática asignadas mediante el ACUERDO PCSJA20-11603 del 27/07/2020, relacionadas con la gestión de seguridad de la información en la Rama Judicial son:

1. Asegurar la operación eficiente de la infraestructura de los sistemas informáticos de la Rama Judicial, incluyendo la infraestructura de software (sistemas operacionales, bases de datos, ambientes de desarrollo y pruebas, ambientes de virtualización, ambientes de producción, empaquetadores de software como contenedores y librerías; herramientas de software para optimizar la arquitectura técnica de la infraestructura como herramientas de integración, autenticación, seguridad; herramientas de software de productividad para usuarios y para programadores, y en general todos los ambientes de software requeridos por las diferentes aplicaciones o paquetes que se usan en la Rama Judicial), la infraestructura de hardware (servidores, computadores personales, impresoras, escáneres, equipos de grabación de audiencias, equipos conexos requeridos en los despachos), las comunicaciones (redes LAN, conectividad vía internet, redes WAN), los centros de datos (propios, nubes privadas, nubes públicas), y los servicios relacionados (soporte y mantenimiento de la infraestructura), de acuerdo con las directrices del Director Ejecutivo de Administración Judicial, las políticas y lineamientos del Consejo Superior de la Judicatura.
2. Implementar las políticas, procesos, productos y servicios de seguridad de la información y seguridad informática en la operación de los sistemas informáticos establecidas por las instancias encargadas de la Seguridad de la Información y la Seguridad Informática en coordinación con el Grupo de Proyectos Especiales de Tecnología.

Cabe aclarar que se han llevado a cabo diagnósticos en la Rama Judicial, que tienen que ver con la Gestión de la Seguridad de la Información, donde se han hecho recomendaciones importantes, como las realizadas por el Banco Mundial en el documento “Plan Estratégico de Seguridad de la Información y Ciberseguridad”. De acuerdo con lo mencionado anteriormente se proponen los siguientes roles y responsabilidades para el Sistema de Gestión de Seguridad de la Información, Ciberseguridad y Protección de Datos Personales de la Rama Judicial:

* + 1. Normograma

| **Rol** | **Responsabilidades** | **Autoridades** |
| --- | --- | --- |
| ALTA DIRECCIÓN | - Lidera el diseño, implementación y mantenimiento del Sistema de Gestión de Seguridad de la Información.  - Define la política y objetivos de Seguridad de la información.  - Define los planes y estrategias de carácter operativo para alcanzar los objetivos en seguridad de la información.  - Evalúa y revisa el cumplimiento de los objetivos del Sistemas de Gestión de seguridad de la Información.  - Revisa periódicamente la plataforma estratégica del Sistema de Gestión de Seguridad de la Información. | - Aprueba y revisa la política y objetivos de Seguridad de la Información.  - Aprueba y ajusta los planes y estrategias de operación.  - Solicita revisiones y auditorías del sistema de Gestión de Seguridad de la Información. |
| REPRESENTANTE DE LA ALTA DIRECCIÓN (DIRECTOR EJECUTIVO DE ADMINISTRACIÓN JUDICIAL) | - Plantea las directrices y estrategias necesarias para garantizar el diseño, implementación, sostenimiento y mejoramiento del Sistema Gestión Seguridad de la Información “SGSI-SIGCMA”.  - Propende por el cumplimiento de la política y objetivos de seguridad de la Información.  - Asegura que se establezcan y mantengan los procesos necesarios para el Sistema de Gestión de Seguridad de la Información.  - Asegura que se promueva la toma de conciencia de los requisitos del cliente en los empleados y todos los funcionarios y servidores judiciales al Sistema de Gestión de Seguridad de la Información.  - Representa a la alta dirección en todas las relaciones con partes externas sobre el sistema de gestión de Seguridad de la Información.  - Informa a la alta dirección sobre el desempeño del Sistema de Gestión de Seguridad de la Información y de sus necesidades. | - Solicita la toma de acciones de gestión cuando lo considere necesario.  - Promueve revisiones y auditorías del Sistema de Gestión de Seguridad de la Información cuando lo considere necesario. |
| GRUPO DE PROYECTOS ESPECIALES DE TECNOLOGÍA (GPET) | - Propende por el cumplimiento de la Política y los Objetivos de Seguridad de la Información.  - Lidera y desarrolla las políticas y estrategias definidas por la Alta Dirección.  - Informa permanentemente a la Alta Dirección sobre el estado y desempeño del Sistema.  - Revisa, ajusta y presenta anualmente a la Alta Dirección los planes de mantenimiento, mejoramiento y el plan de comunicaciones, y realiza su correspondiente seguimiento.  - Revisa y evalúa periódicamente el Sistema de Calidad, garantizando su eficiencia, eficacia y efectividad. | - Toma decisiones para garantizar la implementación, mantenimiento y mejora del Sistema De Gestión De Seguridad de la Información. |
| COMITÉ DEL SIGCMA | - Revisa y aprueba las propuestas sobre creación, modificación o anulación de la documentación del Sistema de Gestión de Calidad. | - Aprueba la creación modificación y mejora de la documentación del Sistema De Gestión De Seguridad de la Información. |
| COORDINADOR DEL SIGCMA | - Coordina las actividades de comunicaciones y documentación.  - Presta apoyo técnico y metodológico a las diferentes instancias en la implementación y mantenimiento del Sistema de Gestión de Seguridad de la Información.  - Convoca y asiste en Calidad de relator a las reuniones ordinarias y extraordinarias del comité del Sistema de Gestión de Seguridad de la Información.  - Proyecta anualmente el plan de mantenimiento y mejoramiento del Sistema de Gestión de Seguridad de la Información lo presenta al Comité de Calidad para su revisión.  - Consolida el informe de revisión por proceso para la alta dirección.  - Realiza en Coordinación de los Líderes de los procesos el seguimiento al funcionamiento de los equipos operativos de los procesos.  - Evalúa técnicamente la pertinencia de las acciones correctivas, preventivas y de  mejora y hace seguimiento a su cumplimiento.  - Verifica periódicamente la aplicación de los procedimientos de mejoramiento continuo.  - Administra los listados maestros de las acciones de gestión. | - Revisa y avala las actividades de mejoramiento, comunicaciones y documentación del Sistema de Gestión de Calidad |
| COORDINADOR DE DOCUMENTACIÓN | - Verifica la implementación y cumplimiento de los procedimientos para el control de documentos internos, externos y registros.  - Pública los documentos aprobados por el Sistema de Gestión de Seguridad de la Información, con el fin de garantizar la disponibilidad de los mismos para todos los servidores del Sistema de Gestión de Seguridad de la Información.  - Presta asesoría para la elaboración, implementación o mejoramiento de la documentación del Sistema de Gestión de Calidad.  - Reporta a la Coordinación de Calidad, los resultados de las actividades que se lleven a cabo por la Coordinación de Documentación. | - Coordinar, asesorar y acompañar las actividades de diseño, implementación, sostenimiento y mejoramiento del Sistema de gestión Documental del SICGMA |

* + 1. Comité de Seguridad de la Información

El Comité de Seguridad de la Información determina la estrategia de desarrollo y evolución del Sistema de Gestión de Seguridad y Ciberseguridad. Así mismo decide la asignación de los recursos necesarios para alcanzar los objetivos establecidos y desempeña una función de vigilancia.

Son miembros permanentes los siguientes:

* Por lo menos un representante de la Presidencia del CSJ.
* Un representante de la Coordinación Nacional de Calidad.
* Un representante de la Unidad de Auditoria.
* Por lo menos un representante de la Unidad de Informática.
* Por lo menos un representante del Grupo de Proyectos Especiales de Tecnología.
* Oficial de Seguridad de la Información.

Los siguientes Servidores Judiciales tendrán presencia en el comité de seguridad de forma itinerante:

* Un representante de la Corte Suprema de Justicia.
* Un representante del Consejo de Estado.
* Un representante de la Corte Constitucional.
* Un representante de la Comisión Nacional de Disciplina Judicial.
* Un representante de los Consejos Seccionales de la Judicatura.

**Nota:** La presidencia de cada corporación designará su representante en el Comité de Seguridad de la Información, y tendrá voz y voto para su jurisdicción.

Las funciones del Comité de Seguridad de la Información son:

* Asignar los recursos necesarios para el cumplimiento de los objetivos del SGSI.
* Revisar periódicamente las políticas de Seguridad de la Información, Ciberseguridad y Protección de Datos Personales con el fin de mantenerlas actualizadas, vigentes, operativas para asegurar su permanencia y nivel de eficacia.
* Aprobar iniciativas para incrementar la seguridad de la información, la ciberseguridad y la protección de los datos personales.
* Acompañar e impulsar el desarrollo de proyectos en pro de la Seguridad de la Información, Ciberseguridad y Protección de Datos Personales en la Rama Judicial.
* Aprobar el uso de metodologías y procesos específicos para la seguridad y privacidad de la información.
* Promover la difusión y sensibilización de la seguridad de la información en la Rama Judicial.
  + 1. Oficina de Seguridad de la Información

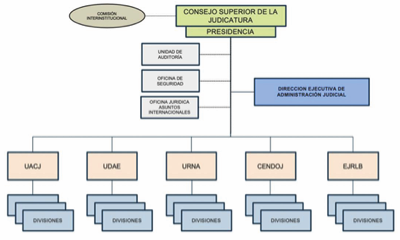
El objetivo principal de la Oficina de Seguridad de la Información es asegurar el cumplimiento de las políticas y procedimientos de seguridad, ciberseguridad y privacidad de la información en la Rama Judicial, para esto cuenta con el posicionamiento y la autoridad, libre de conflicto de intereses. La Oficina de Seguridad de la Información reporta directamente al CSJ a través del Grupo de Proyectos Especiales de Tecnología – GPET.

Las funciones de la Oficina de Seguridad de la Información son:

* Coordinar la implementación, mantenimiento y mejora continua del Sistema de Gestión de Seguridad de la Información, Ciberseguridad y Protección de Datos Personales con base en las mejores prácticas y siguiendo los lineamientos de MINTIC.
* Asegurar, proteger, gestionar y clasificar los activos de información de la Rama Judicial.
* Definir y poner en marcha la metodología para la identificación, evaluación y análisis de riesgos de Seguridad de la Información, Ciberseguridad y Protección de Datos Personales y liderar el plan para su tratamiento.
* Establecer los lineamientos para la configuración de las herramientas de seguridad informática para la gestión de vulnerabilidades, riegos e incidentes de seguridad.
* Fortalecer el proceso de gestión de vulnerabilidades en los sistemas de información del CSJ y proponer planes de remediación.
* Proponer controles y procedimientos para gestionar incidentes de seguridad, fugas de información y coordinar la respuesta oportuna en conjunto con la Unidad Informática.
* Liderar la definición del Plan de Continuidad del Negocio (BCP) y Recuperación Tecnológica (DRP), su implementación y pruebas periódicas al interior del CSJ.
* Generar indicadores y métricas de Seguridad de la Información, Ciberseguridad y Protección de Datos Personales, tanto a nivel técnico como a nivel estratégico.
* Proponer estrategias para la sensibilización y concientización de la importancia de la Seguridad de la Información, Ciberseguridad y Protección de Datos Personales.
* Atender las observaciones y hallazgos de las auditorías internas de control sobre la Seguridad de la Información, Ciberseguridad y Protección de Datos Personales
* Atender los requerimientos de Seguridad de la Información, Ciberseguridad y Protección de Datos Personales establecidos por MINTIC y el Gobierno Nacional.

La Oficina de Seguridad de la Información tiene Nivel de Asesor, esto con el fin de que reporte directamente al CSJ. Esto le garantiza el posicionamiento y la autoridad para hacer que se cumplan las políticas y procedimientos de seguridad de la información en toda la Rama Judicial.

En la ilustración 6, se presenta la ubicación de la oficina de seguridad dentro de la jerarquía del CSJ:



Aquí está la OSI

**Ilustración 7. Ubicación de la Oficina de Seguridad de la Información**

La estructura de la Oficina de Seguridad de la Información está conformada por un Director de Seguridad de la Información, un Oficial de Seguridad de la Información, una División de Seguridad de la Información, una División de Ciberseguridad y una División de Protección de Datos Personales:



**Ilustración 8. Estructura de la Oficina de Seguridad de la Información**

* + 1. Director de la Oficina de Seguridad de la Información

El director de la Oficina de Seguridad de la Información es el encargado de alinear los objetivos y las iniciativas de seguridad de la información y ciberseguridad con los objetivos estratégicos y proyectos del CSJ. El director de la Oficina de Seguridad de la Información tiene las siguientes funciones:

* Liderar las operaciones de la Oficina de Seguridad de la Información y su coordinación e interacción con las demás áreas del CSJ.
* Generar e implementar políticas para garantizar la seguridad y privacidad de la información, así como para la gestión de riesgos.
* Revisar y aprobar el Sistema de Gestión de Seguridad de la Información, Ciberseguridad y Protección de Datos Personales.
* Proponer estrategias para la sensibilización en seguridad de la información y campañas para la apropiación del Sistema de Gestión de Seguridad de la Información, Ciberseguridad y Protección de Datos Personales en la Rama Judicial.
* Coordinar las iniciativas y actividades de ciberseguridad con la UI para la gestión de vulnerabilidades, riegos e incidentes de seguridad.
* Hay que asegurar que los activos de información del CSJ estén protegidos.
* Establecer y mantener un sistema de monitoreo de los niveles de conformidad en el manejo de datos e información del CSJ.
* Estructurar y mantener una infraestructura adecuada para la gestión de seguridad y privacidad de la información en el CSJ.
* Asegurar la continuidad de la seguridad de la información, garantizando su inclusión en el alcance del BCP y el DRP, así como en las pruebas correspondientes.
* Estar al tanto de la evolución de las amenazas cibernéticas y explorar las nuevas tecnologías que las puedan contrarrestar.
  + 1. Oficial de Seguridad de la Información

El Oficial de Seguridad de la Información tiene asignadas las siguientes responsabilidades:

* Responsable de establecer, implementar, mantener y mejorar continuamente el Sistema de Gestión de Seguridad de la Información, Ciberseguridad y Protección de Datos Personales.
* Verifica que el Sistema de Gestión de Seguridad de la Información, Ciberseguridad y Protección de Datos Personales, cuente con los procedimientos, formatos y herramientas necesarias para su correcta implementación dentro de la Rama Judicial.
* Coordina la realización de un análisis de riesgos de Seguridad de la Información, Ciberseguridad y Protección de Datos Personales en cada una de las corporaciones incluidas en el alcance del SGSI. Este análisis debe llevarse a cabo como mínimo una vez al año, con el fin de determinar el grado de exposición de los activos y contenedores de información a las amenazas internas y externas de la Rama Judicial.
* Difunde y controla la aplicación e implementación de las políticas de Seguridad de la Información, Ciberseguridad y Protección de Datos Personales, con el fin de garantizar su cumplimiento.
* Prepara el plan de formación y sensibilización para la Seguridad de la Información, Ciberseguridad y Protección de Datos Personales.
* Mantiene el inventario de activos de la Información actualizado.
* Evalúa los riesgos de Seguridad de la Información, Ciberseguridad y Protección de Datos Personales relacionados con las actividades subcontratadas.
* Controla la efectividad de los controles implementados.
* Vela por la implementación de auditorías internas para verificar el cumplimiento de las Políticas de Seguridad de la Información, Ciberseguridad y Protección de Datos Personales.
* Presentar a la alta dirección los reportes con el avance de implementación del SGSI y Ciberseguridad, así como los incidentes materializados y su tratamiento.
* Atender los requerimientos de seguridad de la información establecidos por MINTIC y el Gobierno Nacional.
  + 1. Coordinador de Protección de Datos Personales

El Coordinador de Protección de Datos Personales tiene asignadas las siguientes responsabilidades:

* Proteger los datos personales y dar trámite a las solicitudes de los Titulares de los datos personales para el ejercicio de los derechos que se consagran en la ley 1581 de 2012.
* Servir de coordinador con las demás áreas de la organización para asegurar una implementación transversal de la Responsabilidad Demostrada.
* Mantener un inventario de las bases de datos personales en poder de la Rama Judicial y clasificarlas según su contenido.
* Registrar las bases de datos de la Rama Judicial en el Registro Nacional de Bases de Datos cuando corresponda, y actualizar el reporte atendiendo a las instrucciones que sobre el particular emita la Superintendencia de Industria y Comercio (SIC).
* Implementar en los contratos que celebre la Rama Judicial, disposiciones que aseguren el cumplimiento de la Ley 1581 de 2012.
* Velar porque se capacite periódicamente en temas de protección de datos personales a los servidores judiciales y proveedores de la Rama Judicial, para generar una cultura de protección de datos dentro en las corporaciones incluidas en el alcance del SGSI. Esto incluye realizar capacitaciones, medir la participación y calificar el desempeño de los asistentes.
* Integrar las políticas de datos dentro de las actividades de las demás unidades del CSJ y corporaciones incluidas en el alcance del SGSI.
* Presentar a la alta dirección los reportes con el avance de implementación del programa de protección de datos personales, así como cualquier evento o incidente que se presente con respecto a los datos personales.
* Las demás tareas que les sean asignadas relacionadas con la implementación y mantenimiento de las iniciativas de Protección de Datos Personales.
  + 1. Coordinador de Ciberseguridad

El Coordinador de Ciberseguridad tiene asignadas las siguientes responsabilidades:

* Coordinar las iniciativas de ciberseguridad en la Rama Judicial.
* Establecer los lineamientos para la configuración de las herramientas de seguridad informática para la gestión de vulnerabilidades, riesgos e incidentes de seguridad.
* Coordinar el proceso de gestión vulnerabilidades en los sistemas de información de la Rama Judicial y proponer planes de remediación.
* Proponer controles y procedimientos para gestionar incidentes de seguridad y fugas de información y coordinar la respuesta oportuna en conjunto con la UI.
* Genera indicadores, métricas y metas de ciberseguridad, tanto a nivel técnico como a nivel estratégico y medir periódicamente los mismos.
* Las demás tareas que les sean asignadas relacionadas con la implementación y mantenimiento de las iniciativas de Ciberseguridad.
  + 1. Coordinador de Seguridad de la Información

El Coordinador de Ciberseguridad tiene asignadas las siguientes responsabilidades:

* Coordinar la implementación, mantenimiento y mejora continua del SGSI con base en las mejores prácticas y siguiendo los lineamientos del MINTIC.
* Coordinar la implementación de las políticas de seguridad de la información en la Rama Judicial.
* Definir y poner en marcha la metodología para la identificación, clasificación y valoración de activos de información.
* Definir y poner en marcha la metodología para la identificación, evaluación y análisis de riesgos y apoyar la definición de los planes de tratamiento.
* Generar indicadores, métricas y metas de seguridad de la información, tanto a nivel técnico como a nivel estratégico y medir periódicamente los mismos.
* Proponer estrategias para la sensibilización y concientización sobre la importancia de la seguridad, la privacidad de la información y la apropiación del SGSI.
* Las demás tareas que les sean asignadas relacionadas con la implementación y mantenimiento de las iniciativas de Seguridad de la Información.
  + 1. Analistas de Ciberseguridad

Los Analistas de Ciberseguridad tienen asignadas las siguientes responsabilidades:

* Apoyar las iniciativas de ciberseguridad en la Rama Judicial.
* Apoyar la definición de lineamientos para la configuración de las herramientas de seguridad informática para la gestión de vulnerabilidades, riesgos e incidentes de seguridad.
* Apoyar el proceso de gestión vulnerabilidades en los sistemas de información de la Rama Judicial y proponer planes de remediación.
* Apoyar la propuesta para la definición de controles y procedimientos para gestionar incidentes de seguridad y fugas de información.
* Apoyar la elaboración de indicadores, métricas y metas de ciberseguridad, tanto a nivel técnico como a nivel estratégico y la medición periódica de los mismos.
* Las demás tareas que les sean asignadas relacionadas con la implementación y mantenimiento de las iniciativas de Ciberseguridad.
  + 1. Analistas de Seguridad de la Información

Los Analistas de Seguridad de la Información tienen asignadas las siguientes responsabilidades:

* Apoyar la implementación, mantenimiento y mejora continua del SGSI con base en las mejores prácticas y siguiendo los lineamientos del MINTIC.
* Apoyar la implementación de las políticas de seguridad de la información de la Rama Judicial.
* Apoyar la puesta en marcha de la metodología para la identificación, clasificación y valoración de activos de información.
* Apoyar la puesta en marcha de la metodología para la identificación, evaluación y análisis de riesgos y planes de tratamiento
* Apoyar la elaboración de indicadores, métricas y metas de seguridad de la información, tanto a nivel técnico como a nivel estratégico y la medición periódica de los mismos.
* Apoyar la elaboración de estrategias para la sensibilización y concientización sobre la importancia de la seguridad, privacidad de la información y la apropiación del SGSI.
* Las demás tareas que les sean asignadas relacionadas con la implementación y mantenimiento de las iniciativas de Seguridad de la Información.
  + 1. Líderes de proceso

Los Lideres de Proceso tienen las siguientes funciones:

* Generar conciencia al interior de las unidades de la Rama Judicial, la importancia del Sistema de Gestión de Seguridad de la Información, Ciberseguridad y Protección de Datos Personales.
* Responsables de gestionar los riesgos y hacer seguimiento.
  + 1. Servidores Judiciales
* Responsables de ejecutar controles operativos en el día a día, relacionados con la Seguridad de la Información, Ciberseguridad y Protección de Datos Personales.
* Notificar cualquier evento o incidente relacionados con la Seguridad de la Información, Ciberseguridad y Protección de Datos Personales a través de los canales definidos.
  + 1. Auditoría Interna o Externa
* Llevar a cabo auditorías al Sistema de Gestión de Seguridad de la Información, Ciberseguridad y Protección de Datos Personales, de manera que se garantice su idoneidad, y eficiencias adecuadas.

1. PLANIFICACIÓN
   1. Acciones para tratar riesgos y oportunidades
      1. Generalidades

Durante la planificación del Sistema de Gestión de Seguridad de la Información, Ciberseguridad y Protección de Datos Personales, se deben considerar los riesgos y oportunidades con el fin de:

* 1. Asegurar que el Sistema de Gestión de Seguridad de la Información, Ciberseguridad y Protección de Datos Personales pueda conseguir los resultados previstos.
  2. Prevenir o reducir efectos indeseados.
  3. Lograr la mejora continua.

Los riesgos a los que se hace referencia son riesgos relacionados con:

* La definición del alcance del Sistema de Gestión de Seguridad de la Información, Ciberseguridad y Protección de Datos Personales.
* El cumplimiento de los objetivos del Sistema de Gestión de Seguridad de la Información, Ciberseguridad y Protección de Datos Personales.
* El compromiso de la alta dirección respecto con el Sistema de Gestión de Seguridad de la Información, Ciberseguridad y Protección de Datos Personales.
* Los recursos para operar el Sistema de Gestión de Seguridad de la Información, Ciberseguridad y Protección de Datos Personales.

Mientras que las oportunidades a las que se hace referencia están relacionadas con:

* El resultado del Sistema de Gestión de Seguridad de la Información, Ciberseguridad y Protección de Datos Personales.
* El valor del Sistema de Gestión de Seguridad de la Información, Ciberseguridad y Protección de Datos Personales para la Rama Judicial, a nivel de costo / beneficio.
* El beneficio de asegurar la operación de los procesos gracias al Sistema de Gestión de Seguridad de la Información, Ciberseguridad y Protección de Datos Personales.
* Perfeccionar procesos o eliminar procesos que no son rentables.
* Introducción de nuevas tecnologías de la información.

Para llevar a cabo el análisis de riesgos y oportunidades se recomienda utilizar el análisis FODA, que es una herramienta que permite conformar un cuadro de la situación actual del Sistema de Gestión de Seguridad de la Información, Ciberseguridad y Protección de Datos Personales, permitiendo de esta manera obtener un diagnóstico preciso que permite, tomar decisiones para prevenir riesgos y garantizar el cumplimiento de los objetivos del sistema de gestión, tal como se presenta en la ilustración 8, a continuación:

Factores internos (Fortalezas, Debilidades)

Factores externos (Oportunidades, Amenazas)

**Ilustración 9. Matriz FODA**

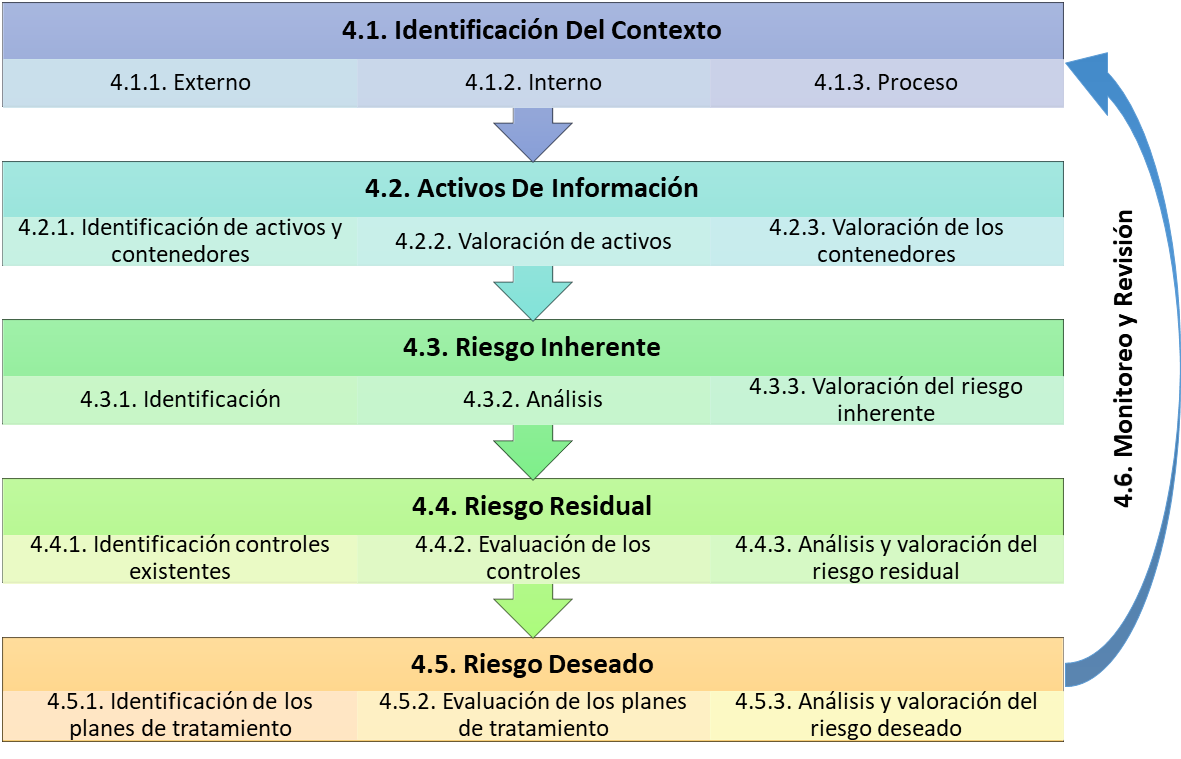
* + **Fortalezas:** Son las capacidades especiales con que cuenta la Rama Judicial, y que le permiten el cumplimiento de los objetivos del Sistema de Gestión de Seguridad de la Información, Ciberseguridad y Protección de Datos Personales. Recursos que se controlan, capacidades y habilidades que se poseen, actividades que se desarrollan positivamente, etc.
  + **Oportunidades:** Son aquellos factores que resultan positivos, favorables, explotables, que se deben descubrir en el entorno en el que opera el Sistema de Gestión de Seguridad de la Información, Ciberseguridad y Protección de Datos Personales, y que permiten garantizar el cumplimiento de sus objetivos.
  + **Debilidades:** Son aquellos factores que provocan una posición desfavorable para el Sistema de Gestión de Seguridad de la Información, Ciberseguridad y Protección de Datos Personales. Recursos de los que se carece, habilidades que no se poseen, actividades que no se desarrollan positivamente, etc.
  + **Amenazas:** Son aquellas situaciones que provienen del entorno y que pueden llegar a atentar contra el cumplimiento de los objetivos del Sistema de Gestión de Seguridad de la Información, Ciberseguridad y Protección de Datos Personales.

El resultado del análisis FODA del SGSI de la Rama Judicial llevado a cabo en abril de 2022, se presenta en el Anexo B “[Matriz FODA](https://etbcsj.sharepoint.com/teams/Proyecto166-2021SGSI/Documentos%20compartidos/General/SGSI/02%20-%20Etapa%20de%20Ejecución/06%20-%20DOCUMENTOS%20REVISIÓN/Estructura%20ISO%2027001%20V2/2.%20Planear%20-%20Numerales%204,%205,%206%20y%207/MATRIZ%20DOFA.xlsm)”.

Adicionalmente, se incluye un plan de ruta en el Anexo C, que tiene como fin presentar los hitos más relevantes para garantizar que el Sistema de Gestión de Seguridad de la Información, Ciberseguridad y Protección de Datos Personales cumpla su propósito en la Rama Judicial.

* + 1. Identificación y Valoración de Riesgos de Seguridad de la Información

La Rama Judicial establece mediante la “[Metodología de Gestión de Activos y Riesgos de Seguridad de la Información](https://etbcsj.sharepoint.com/teams/Proyecto166-2021SGSI/Documentos%20compartidos/General/SGSI/02%20-%20Etapa%20de%20Ejecución/06%20-%20DOCUMENTOS%20REVISIÓN/Estructura%20ISO%2027001%20V2/2.%20Planear%20-%20Numerales%204,%205,%206%20y%207/Metodología%20Gestión%20Activos%20Riesgos%20Seguridad%20Informacion.docx)” los criterios para ejecutar cada una de las etapas señaladas en la norma ISO 31000:2018, es decir la contextualización, identificación, análisis, evaluación y tratamiento del riesgo. Así mismo, establece las pautas para identificar activos de información, los cuales son la base para identificar y gestionar los riesgos de Seguridad de la Información, Ciberseguridad y Protección de Datos Personales. La metodología se compone de los pasos que se presentan en la ilustración 9, a continuación:



**Ilustración 10. Metodología de gestión de riesgos integrada**

El análisis de riesgos de Seguridad de la Información, Ciberseguridad y Protección de Datos Personales debe llevarse a cabo como mínimo una vez al año o cada vez que se presenten cambios significativos que pueden afectar la valoración de los riesgos identificados.

* + 1. Tratamiento de Riesgos de seguridad de la información

Consiste en identificar los planes de tratamiento más adecuados para los riesgos identificados en la Rama Judicial. Esto implica equilibrar los costos, esfuerzos y beneficios de su implementación.

En el documento “[Metodología de Gestión de Activos y Riesgos de Seguridad de la Información](https://etbcsj.sharepoint.com/teams/Proyecto166-2021SGSI/Documentos%20compartidos/General/SGSI/02%20-%20Etapa%20de%20Ejecución/06%20-%20DOCUMENTOS%20REVISIÓN/Estructura%20ISO%2027001%20V2/2.%20Planear%20-%20Numerales%204,%205,%206%20y%207/Metodología%20Gestión%20Activos%20Riesgos%20Seguridad%20Informacion.docx)” se establecen los criterios de aceptación del riesgo[[2]](#footnote-3), aquellos riesgos que no son tolerados o aceptables por la Rama Judicial deben contar con planes de tratamiento que mitiguen la probabilidad o el impacto de este. Dicho plan debe definirse mediante el proceso para el tratamiento del riesgo que incluye opciones, como: Reducir, Evitar, Transferir, o Aceptar el riesgo. Lo anterior con el fin de llevar los riesgos a un nivel aceptable.

Una vez han sido evaluadas las opciones para el tratamiento del riesgo, se seleccionan aquellas cuyo costo / beneficio sea el más adecuado para la Rama Judicial y se define su plan de implementación.[[3]](#footnote-4)

* 1. Objetivos del Sistema de Gestión de Seguridad de la Información, Ciberseguridad y Protección de Datos Personales para la Rama Judicial

A continuación, los objetivos definidos para el SGSI en la vigencia de 2022:

* + 1. Seguridad de la Información:

1. Gestionar de manera eficaz los recursos asignados al Sistema de Gestión de Seguridad de la Información, Ciberseguridad y Protección de Datos Personales para que logre los resultados propuestos en la Rama Judicial.
2. Fortalecer la cultura de Seguridad de la Información, Ciberseguridad y Protección de Datos Personales en la Rama Judicial.
3. Proteger, preservar y administrar los activos de información junto con las tecnologías utilizadas para su procesamiento, almacenamiento y transmisión, frente a amenazas internas o externas, con el fin de asegurar la confidencialidad, la integridad y disponibilidad, de manera coordinada con las partes interesadas.
4. Identificar y clasificar los activos y contenedores de información de la Rama Judicial.
5. Disponer de contingencias con el fin de asegurar la continuidad en la prestación de los servicios tecnológicos frente a los incidentes de Seguridad de la Información, Ciberseguridad y Protección de Datos Personales, que se puedan llegar a presentar.
6. Implementar y operar un modelo que permita gestionar adecuadamente los incidentes de Seguridad de la Información, Ciberseguridad y Protección de Datos Personales que se puedan presentar en la Rama Judicial.
7. Minimizar las vulnerabilidades técnicas en las plataformas tecnológicas que prestan servicios transversales a la Rama Judicial, mediante un ejercicio periódico de monitoreo, revisión, mitigación y validación de que las mismas han sido efectivamente corregidas.
8. Verificar y garantizar el cumplimiento de las políticas definidas como parte del Sistema de Gestión de Seguridad de la Información, Ciberseguridad y Protección de Datos Personales.
9. Aplicar un proceso de gestión de riesgos de Seguridad de la Información, Ciberseguridad y Protección de Datos Personales con el fin de identificar, analizar, evaluar y tratar los riesgos asociados con la pérdida de la confidencialidad, de integridad y de disponibilidad de la información.
10. Establecer las acciones preventivas y correctivas, de acuerdo con los resultados de la revisión por las instancias establecidas, garantizando la mejora continua del Sistema de Gestión de Seguridad de la Información, Ciberseguridad y Protección de Datos Personales.
11. Definir políticas y procedimientos para dar cumplimiento a las disposiciones generales de protección de datos personales establecidas en la Ley 1581 de 2012.

Los indicadores de gestión que permiten medir el cumplimiento de los objetivos del SGSI se pueden observar en el documento “[Indicadores SGSI](https://etbcsj.sharepoint.com/teams/GrupoCertificacin27001DEAJ/Documentos%20compartidos/General/Indicadores/Indicadores%20SGSI.xlsx)” y a través del Manual de Protección de Datos Personales y sus procedimientos correspondientes.

1. SOPORTE
   1. Recursos

El comité de seguridad de la información aprueba la política del Sistema de Gestión de Seguridad de la Información, Ciberseguridad y Protección de Datos Personales para la Rama Judicial, como muestra de su compromiso y apoyo en el diseño e implementación de políticas eficientes que garanticen la confidencialidad, integridad y disponibilidad de la información en las corporaciones incluidas en el alcance del SGSI. Adicionalmente, demuestran su compromiso mediante las siguientes actividades:

* Revisar, aprobar y garantizar la divulgación de las Políticas de Seguridad de la Información, Ciberseguridad y Protección de Datos Personales.
* Concienciación para generar cultura en Seguridad de la Información, Ciberseguridad y Protección de Datos Personales en la Rama Judicial.
* Garantizar los recursos adecuados para implementar y mantener las Políticas de Seguridad de la Información, Ciberseguridad y Protección de Datos Personales.
* Verificar el cumplimiento de las Políticas de Seguridad de la Información, Ciberseguridad y Protección de Datos Personales.
* Asegurar que los procedimientos de seguridad brinden apoyo a los requisitos de la Rama Judicial
* Identificar y entender los requisitos legales y reglamentarios.
* Mantener la seguridad suficiente mediante la aplicación correcta de todos los controles requeridos.
* Llevar a cabo revisiones cuando sea necesario y reaccionar apropiadamente a los resultados de estas revisiones.
* Mejorar el SGSI manteniendo un control y evolución del mismo,
* Garantizar la actualización de la documentación del SGSI (Manuales, Políticas, Procesos, Procedimientos, Gestión de Activos, Gestión de Riesgos, etc.).
  1. Competencia

La Rama Judicial asegurará que los servidores judiciales con responsabilidad en el Sistema de Gestión de Seguridad de la Información, Ciberseguridad y Protección de Datos Personales adquieran la formación, capacitación y las competencias necesarias en seguridad de la información, ciberseguridad y protección de los datos personales según los perfiles definidos mediante los siguientes lineamientos (Ver Anexo D. Perfiles del SGSI):

* Formar y capacitar al personal que desarrolle funciones relacionadas con el Sistema de Gestión de Seguridad de la Información, Ciberseguridad y Protección de Datos Personales para la Rama Judicial.
* Suministrar formación o capacitación para desarrollar programas de sensibilización y generación de cultura en Seguridad de la Información, Ciberseguridad y Protección de Datos Personales.
* Contratar el personal competente para desarrollar programas de capacitación y generación de cultura en Seguridad de la Información, Ciberseguridad y Protección de Datos Personales cuando sea necesario.
* Mantener registros de la formación y capacitación de los involucrados en el Sistema de Seguridad de la Información, Ciberseguridad y Protección de Datos Personales.
* Identificar necesidades de capacitación, formación, sensibilización en Seguridad de la Información, Ciberseguridad y Protección de Datos Personales durante la operación del sistema.
  1. Toma de Conciencia

La Rama Judicial garantizará que se lleven a cabo campañas de concientización y sensibilización a los servidores judiciales, proveedores y usuarios en general respecto a la política del Sistema de Gestión de Seguridad de la Información, Ciberseguridad y Protección de Datos Personales, así como la importancia de su contribución a la eficacia del sistema de gestión, los beneficios que trae para las corporaciones incluidas en el alcance del SGSI y las repercusiones de las no conformidades identificadas por el no cumplimiento de los lineamientos establecidos, garantizando de esta forma una mejora continua del sistema en mención, y logrando su madurez en el tiempo.

* 1. Comunicación

La Rama Judicial, cuenta con el documento “[Plan de Comunicaciones del Sistema de Gestión de Seguridad de la Información, Ciberseguridad y Protección de Datos Personales](https://etbcsj.sharepoint.com/teams/Proyecto166-2021SGSI/Documentos%20compartidos/General/SGSI/02%20-%20Etapa%20de%20Ejecución/06%20-%20DOCUMENTOS%20REVISIÓN/Estructura%20ISO%2027001%20V2/2.%20Planear%20-%20Numerales%204,%205,%206%20y%207/Plan%20de%20Comunicaciones%20SGSI.docx)”, en el cual se define:

* Necesidades de comunicación: En el cual se establece la sombrilla comunicacional, la metodología comunicacional y la medición de la estrategia comunicacional.
* Público objetivo y temas de las campañas en Seguridad de la Información, Ciberseguridad y Protección de Datos Personales.
* Cronograma de las actividades a realizar.

La finalidad de este plan es garantizar la correcta divulgación de las diferentes campañas en términos de Seguridad de la Información, Ciberseguridad y Protección de Datos, logrando así dar cumplimiento a lo requerido por las normas ISO 27001:2013, ISO 27032:2012, la ley 1581 y ley 1712, en relación a que todo el personal debe conocer las políticas y los lineamientos establecidos en el Sistema de Gestión de Seguridad de la Información, Ciberseguridad y Protección de Datos Personales para la Rama Judicial.

* 1. Control Documental

La documentación del Sistema de Gestión de Seguridad de la Información, Ciberseguridad y Protección de Datos Personales, se desarrolló siguiendo la estructura documental establecida en el Sistema Integrado Gestión de Calidad y Medio Ambiente (SIGCMA), lo que permite a la Rama Judicial asegurar el control sobre la creación, aprobación, distribución, utilización y actualización de los documentos y registros utilizados en el Sistema de Gestión de Seguridad de la Información, Ciberseguridad y Protección de Datos Personales.

Los documentos que se originan a partir de este Manual se relacionan a continuación:

* [**Glosario del SGSI**](https://etbcsj.sharepoint.com/teams/Proyecto166-2021SGSI/Documentos%20compartidos/General/SGSI/02%20-%20Etapa%20de%20Ejecución/06%20-%20DOCUMENTOS%20REVISIÓN/Estructura%20ISO%2027001%20V2/2.%20Planear%20-%20Numerales%204,%205,%206%20y%207/GLOSARIO%20SGSI.docx)**:** Documento que incluye todos los términos relevantes para el Sistema de Gestión de Seguridad de la Información, Ciberseguridad y Protección de Datos Personales para la Rama Judicial.
* [**Contexto Organizacional:**](https://etbcsj.sharepoint.com/teams/Proyecto166-2021SGSI/Documentos%20compartidos/General/SGSI/02%20-%20Etapa%20de%20Ejecución/06%20-%20DOCUMENTOS%20REVISIÓN/Estructura%20ISO%2027001%20V2/2.%20Planear%20-%20Numerales%204,%205,%206%20y%207/Contexto%20Organizacional%20SGSI.docx)Establece el contexto organizacional de la Rama Judicial con el fin de tener pleno conocimiento de las corporaciones incluidas en el alcance del SGSI, para el diseño, establecimiento, implementación, monitoreo y mejora continua del Sistema de Gestión de Seguridad de la Información, Ciberseguridad y Protección de Datos Personales para la Rama Judicial.
* [**Plan de Gestión de los Interesados:**](https://etbcsj.sharepoint.com/teams/Proyecto166-2021SGSI/Documentos%20compartidos/General/SGSI/02%20-%20Etapa%20de%20Ejecución/06%20-%20DOCUMENTOS%20REVISIÓN/Estructura%20ISO%2027001%20V2/2.%20Planear%20-%20Numerales%204,%205,%206%20y%207/Anexo%20A.%20Plan%20de%20Gestión%20de%20los%20Interesados.xlsx)Presenta la identificación, valoración y planteamiento de estrategias para la gestión de las partes interesadas en el Sistema de Gestión de Seguridad de la Información, Ciberseguridad y Protección de Datos Personales de la Rama Judicial.
* [**Análisis FODA:**](https://etbcsj.sharepoint.com/teams/Proyecto166-2021SGSI/Documentos%20compartidos/General/SGSI/02%20-%20Etapa%20de%20Ejecución/06%20-%20DOCUMENTOS%20REVISIÓN/Estructura%20ISO%2027001%20V2/2.%20Planear%20-%20Numerales%204,%205,%206%20y%207/MATRIZ%20DOFA.xlsm)Análisis de riesgos y oportunidades del Sistema de Gestión de Seguridad de la Información, Ciberseguridad y Protección de Datos Personales.
* [**Plan de Mejoramiento:**](https://etbcsj.sharepoint.com/teams/Proyecto166-2021SGSI/Documentos%20compartidos/General/SGSI/02%20-%20Etapa%20de%20Ejecución/06%20-%20DOCUMENTOS%20REVISIÓN/Estructura%20ISO%2027001%20V2/5.%20Actuar%20-%20Numeral%2010/CSJ%20-%20Plan%20de%20mejoramiento%20del%20SGSI.docx)Hitos más importantes que deben llevarse a cabo durante el 2022 y el 2023 para garantizar que el Sistema de Gestión de Seguridad de la Información, Ciberseguridad y Protección de Datos Personales logre los resultados esperados en la Rama Judicial.
* [**Metodología de Gestión de Activos y Riesgos de Seguridad de la Información:**](https://etbcsj.sharepoint.com/teams/Proyecto166-2021SGSI/Documentos%20compartidos/General/SGSI/02%20-%20Etapa%20de%20Ejecución/06%20-%20DOCUMENTOS%20REVISIÓN/Estructura%20ISO%2027001%20V2/2.%20Planear%20-%20Numerales%204,%205,%206%20y%207/Metodología%20Gestión%20Activos%20Riesgos%20Seguridad%20Informacion.docx)Establece los criterios para ejecutar cada una de las etapas señaladas en la norma ISO 31000, es decir la contextualización, identificación, análisis, evaluación y tratamiento del riesgo. Así mismo, establece las pautas para identificar activos y contenedores de información, los cuales son la base para identificar y gestionar los riesgos de Seguridad de la Información, Ciberseguridad y Protección de Datos Personales.
* [**Declaración de aplicabilidad SOA:**](https://etbcsj.sharepoint.com/teams/Proyecto166-2021SGSI/Documentos%20compartidos/General/SGSI/02%20-%20Etapa%20de%20Ejecución/06%20-%20DOCUMENTOS%20REVISIÓN/Estructura%20ISO%2027001%20V2/2.%20Planear%20-%20Numerales%204,%205,%206%20y%207/SoA_Rama%20Judicial_27002%20v2022.xlsx)Documento en el que se declara los controles del Anexo A de la ISO 27001 qué harán parte del Sistema de Gestión de Seguridad de la Información, Ciberseguridad y Protección de Datos Personales para la Rama Judicial.
* **Perfiles del SGSI:** Descripción de los perfiles, capacidades y experiencia de los involucrados en el Sistema de Gestión de Seguridad de la Información, Ciberseguridad y Protección de Datos Personales.
* [**Plan de Comunicaciones del Sistema de Gestión de Seguridad de la Información, Ciberseguridad y Protección de Datos Personales:**](https://etbcsj.sharepoint.com/teams/Proyecto166-2021SGSI/Documentos%20compartidos/General/SGSI/02%20-%20Etapa%20de%20Ejecución/06%20-%20DOCUMENTOS%20REVISIÓN/Estructura%20ISO%2027001%20V2/2.%20Planear%20-%20Numerales%204,%205,%206%20y%207/Plan%20de%20Comunicaciones%20SGSI.docx)Establece la sombrilla comunicacional, la metodología comunicacional y la medición de la estrategia comunicacional. Define el público objetivo y temas de las campañas en Seguridad de la Información, Ciberseguridad y Protección de Datos Personales.
* [**Manual de Políticas y Directrices de Seguridad de la Información:**](https://etbcsj.sharepoint.com/teams/Proyecto166-2021SGSI/Documentos%20compartidos/General/SGSI/02%20-%20Etapa%20de%20Ejecución/06%20-%20DOCUMENTOS%20REVISIÓN/Estructura%20ISO%2027001%20V2/3.%20Hacer%20-%20Numeral%208/Controles%20Anexo%20ISO%2027001/Manual%20de%20Politicas/Manual%20Políticas%20SI%20V1.docx)Manual de políticas que tiene como fin dar cumplimiento a los objetivos de control y controles establecidos en el Anexo A de la ISO 27001, con el fin de garantizar buenas prácticas en seguridad de la información y ciberseguridad en la Rama Judicial.
* [**Manual de Protección de Datos Personales:**](https://etbcsj.sharepoint.com/teams/Proyecto166-2021SGSI/Documentos%20compartidos/General/SGSI/02%20-%20Etapa%20de%20Ejecución/06%20-%20DOCUMENTOS%20REVISIÓN/Estructura%20ISO%2027001%20V2/3.%20Hacer%20-%20Numeral%208/Controles%20Anexo%20ISO%2027001/Procedimientos/Manual%20PDP/Manual%20de%20Protección%20de%20Datos%20Personales.docx)Este manual le permite a la Rama Judicial darcumplimiento a la ley 1581 del 2012, en la que se establecen disposiciones para la protección de datos personales.
* [**Indicadores de Gestión:**](https://etbcsj.sharepoint.com/teams/GrupoCertificacin27001DEAJ/Documentos%20compartidos/General/Indicadores/Indicadores%20SGSI.xlsx)Métricas para medir y evaluar el rendimiento y madurez del Sistema de Gestión de Seguridad de la Información, Ciberseguridad y Protección de Datos Personales

1. OPERACIÓN
   1. Planificación y Control Operacional

La Rama Judicial con el apoyo del Comité de Seguridad de la Información se compromete a cumplir lo planeado con respecto al Sistema de Gestión de Seguridad de la Información, Ciberseguridad y Protección de Datos Personales.

La Rama Judicial se compromete a conservar y a controlar la información documentada perteneciente al sistema para garantizar su veracidad.

La Rama Judicial se compromete a controlar los cambios planificados, y a revisar las consecuencias de los cambios no previstos. Si se llegasen a presentar cambios no previstos, se deberá:

* Realizar la evaluación de estos cambios y determinar el nivel de impacto en el SGSI.
* Definir planes con el fin de mitigar los efectos adversos.
* Recolectar y conservar la información documentada sobre el evento.

La Rama Judicial se compromete a asegurar que se identifiquen, y controlen los procesos contratados externamente, mediante el cumplimiento de lo siguiente:

* Hacer seguimiento y revisar los servicios de los proveedores, garantizando que operan de forma adecuada, con el fin de mitigar posibles riesgos futuros.
* Determinar la responsabilidad de este, y tomar las medidas correspondientes en caso de incumplimientos por parte del proveedor.
* Gestionar los cambios correspondientes.

Así mismo, la Rama Judicial se compromete en llevar a cabo auditorías internas y a sus proveedores de manera periódica según lo establecido en el numeral 9.2 de este documento.

Por último, la Rama Judicial se compromete a garantizar la revisión por el Comité de Seguridad de la Información mediante reuniones periódicas con los respectivos integrantes y personal que tenga alguna responsabilidad con respecto al SGSI, con el fin de tratar temas específicos; como lo son los relacionados con el nivel de madurez del sistema, gestión de incidentes, gestión de continuidad, campañas de sensibilización y auditorías internas. De estas reuniones es necesario que se llene un formato de asistencia, dándole así cumplimiento a las normas ISO 27001:2013, ISO 27032:2012, ley 1581 de 2012 y ley 1712 de 2014. Cuando se realice la revisión del Sistema de Gestión de Seguridad de la Información, Ciberseguridad y Protección de Datos Personales por parte del Comité de Seguridad de la información, se deberán ejecutar las acciones identificadas en el numeral 9.3 de este manual.

La Rama Judicial cuenta con un Plan Estratégico de Transformación Digital, que indica las actividades principales a realizar durante entre el 2021 y el 2025, las cuales deben ser ejecutadas dentro de los tiempos planeados para lograr la implementación adecuada del sistema y alcanzar el nivel de madurez “4. Administrado”, según el MSPI.

* 1. Valoración de Riesgos

La Rama Judicial, cuenta con el documento “[*Metodología de Gestión de Activos y Riesgos de Seguridad de la Información*](https://etbcsj.sharepoint.com/teams/Proyecto166-2021SGSI/Documentos%20compartidos/General/SGSI/02%20-%20Etapa%20de%20Ejecución/06%20-%20DOCUMENTOS%20REVISIÓN/Estructura%20ISO%2027001%20V2/2.%20Planear%20-%20Numerales%204,%205,%206%20y%207/Metodología%20Gestión%20Activos%20Riesgos%20Seguridad%20Informacion.docx)*”*, el cual establece los pasos metodológicos para la identificación y valoración de los riesgos de Seguridad de la Información, adicionalmente se establecen los lineamientos necesarios para la gestión adecuada del riesgo, con el fin de garantizar buenas prácticas y de esta manera lograr la mejora continua del Sistema de Gestión de Seguridad de la Información, Ciberseguridad y Protección de Datos Personales para la Rama Judicial.

* 1. Plan de Tratamiento de los Riesgos

La organización cuenta con el documento [“*Metodología de Gestión de Activos y Riesgos de Seguridad de la Información*](https://etbcsj.sharepoint.com/teams/Proyecto166-2021SGSI/Documentos%20compartidos/General/SGSI/02%20-%20Etapa%20de%20Ejecución/06%20-%20DOCUMENTOS%20REVISIÓN/Estructura%20ISO%2027001%20V2/2.%20Planear%20-%20Numerales%204,%205,%206%20y%207/Metodología%20Gestión%20Activos%20Riesgos%20Seguridad%20Informacion.docx)*”*, donde se establecen los pasos metodológicos para el diseño, implementación y puesta en operación de los planes de tratamiento necesarios para mitigar los riesgos existentes en la Rama Judicial.

1. EVALUACIÓN DEL DESEMPEÑO
   1. Seguimiento, Medición, Análisis y Evaluación

La medición de la eficacia al Sistema de Gestión de Seguridad de la Información, Ciberseguridad y Protección de Datos Personales permite identificar oportunidades de mejora que propenden por la evolución del sistema. La medición se desarrolla mediante la gestión de indicadores que miden tanto la eficacia del sistema en general como de los controles implementados.

A continuación, se especifica la aplicación de los indicadores definidos en las diferentes corporaciones de la Rama Judicial:

| Aplicación de los indicadores del SGSI en las diferentes corporaciones de la Rama Judicial: | **Consejo Superior de la Judicatura** | **Corte Suprema de Justicia** | **Consejo de Estado** | **Corte Constitucional** | **Comisión Nacional de Disciplina Judicial** | **Seccional de Bogotá** |
| --- | --- | --- | --- | --- | --- | --- |
| Indicador 1 – Inversión de seguridad de la información | **X** |  |  |  |  |  |
| Indicador 2.1 - Formación | **X** |  |  |  |  |  |
| Indicador 2.2 – Sensibilización | **X** |  |  |  |  |  |
| Indicador 3.1 – Protección de contenedores de información | **X** | **X** | **X** | **X** | **X** | **X** |
| Indicador 3.2 – Activos con análisis de vulnerabilidades | **X** | **X** | **X** | **X** | **X** | **X** |
| Indicador 3.3 – Activos descubiertos | **X** | **X** | **X** | **X** | **X** | **X** |
| Indicador 3.4 – Ejercicios de ethical hacking | **X** | **X** | **X** | **X** | **X** | **X** |
| Indicador 3.5 – Fuentes correlacionadas en Rapid7 | **X** | **X** | **X** | **X** | **X** | **X** |
| Indicador 4 – Actualización de activos de información y BD Personales. | **X** | **X** | **X** | **X** | **X** | **X** |
| Indicador 5 – Continuidad de la seguridad en contingencia | **X** |  |  |  |  |  |
| Indicador 6 - Gestión de incidentes de seguridad de la información. | **X** | **X** | **X** | **X** | **X** | **X** |
| Indicador 7 - Gestión de vulnerabilidad técnica. | **X** |  |  |  |  |  |
| Indicador 8 - Evaluación de cumplimiento de las políticas. | **X** | **X** | **X** | **X** | **X** | **X** |
| Indicador 9 – Implementación de planes de tratamiento. | **X** | **X** | **X** | **X** | **X** | **X** |
| Indicador 10 – Acciones preventivas y correctivas | **X** |  |  |  |  |  |

**Tabla 3. Aplicación de indicadores en las corporaciones de la Rama Judicial**

Adicionalmente para conocer la eficacia del Sistema de Gestión de Seguridad de la Información, Ciberseguridad y Protección de Datos Personales se debe diligenciar anualmente el Instrumento De Identificación De La Línea Base De Seguridad Administrativa Y Técnica – MSPI, para lo cual se cuenta con el procedimiento “[Procedimiento Para El Diligenciamiento De La Instrumento De Identificación De La Línea Base De Seguridad Administrativa Y Técnica – MSP](https://etbcsj.sharepoint.com/teams/Proyecto166-2021SGSI/Documentos%20compartidos/General/SGSI/02%20-%20Etapa%20de%20Ejecución/06%20-%20DOCUMENTOS%20REVISIÓN/Estructura%20ISO%2027001%20V2/4.%20Verificar%20-%20Numeral%209/SGSI%20-%20Procedimiento%20diligenciamiento%20instrumento%20MSPI.docx)I”.

* 1. Auditoria al SGSI
     1. Auditoría Interna

La Rama Judicial, se compromete a llevar a cabo Auditorías Internas, con el fin de obtener información del cumplimiento del Sistema de Gestión de Seguridad de la Información, Ciberseguridad y Protección de Datos Personales para la Rama Judicial, asegurando lo siguiente:

* El sistema mencionado antes se encuentra implementado correctamente.
* Tiene un desempeño acorde a lo esperado.
* Cumplen los requisitos normativos.
* Estas auditorías se encontrarán enmarcadas dentro de un procedimiento que define las responsabilidades y requisitos para la planificación y realización de las mismas, forma y metodología para la presentación de resultados y mantenimiento de los registros.
* Además de los resultados de las auditorías, como entrada a este procedimiento se prevé también la retroalimentación de todos los participantes e involucrados en la operación del sistema, el manejo de no conformidades, medición de los indicadores y sugerencias.

Las auditorías al Sistema de Gestión de Seguridad de la Información, Ciberseguridad y Protección de Datos Personales para la Rama Judicial deben ser realizadas por personal diferente al vinculado con las áreas o procesos que van a ser auditados. Para desarrollar las auditorias se debe seguir el procedimiento establecido en el SGSI “[Procedimiento Auditorías Internas al SGSI](https://etbcsj.sharepoint.com/teams/Proyecto166-2021SGSI/Documentos%20compartidos/General/SGSI/02%20-%20Etapa%20de%20Ejecución/06%20-%20DOCUMENTOS%20REVISIÓN/Estructura%20ISO%2027001%20V2/4.%20Verificar%20-%20Numeral%209/SGSI%20-%20Procedimiento%20Auditorias%20Internas.docx)”.

* + 1. Auditoría Externa

La Rama Judicial, se compromete a llevar a cabo Auditorías Externas al menos una vez al año, las cuales deberán ser realizadas por personal ajeno a la Rama Judicial, con el fin de garantizar independencia y objetividad por tratarse de personal capacitado que no presentan conflictos o intereses con las corporaciones incluidas en el alcance del SGSI.

* 1. Revisión por la Dirección

El Comité de Seguridad de la Información revisará la efectividad de la implementación del Sistema de Gestión de Seguridad de la Información, Ciberseguridad y Protección de Datos Personales para la Rama Judicial, así como el comportamiento de sus indicadores anualmente o cuando se requiera dicha revisión por cambios organizacionales, a nivel de procesos u objetivos estratégicos.

Los temas que serán tratados de forma obligatoria son:

* Revisión de la política y objetivos del sistema de gestión.
* Resultados del análisis de riesgos y seguimiento a los planes de tratamiento establecidos.
* Evaluación de conformidad con los requisitos legales aplicables.
* Estado de análisis e investigación de incidentes de seguridad de la información.
* Resultados de auditorías internas.
* No conformidades.
* Acciones correctivas y preventivas.
* Cambios al Sistema de Gestión de Seguridad de la Información, Ciberseguridad y Protección de Datos Personales para la Rama Judicial.
* Recomendaciones para la mejora.
* Seguimiento de revisiones previas.
* Desempeño financiero y costos relacionados con el sistema.
* Necesidad de recursos.

La revisión por la Dirección del Sistema de Gestión de Seguridad de la Información, Ciberseguridad y Protección de Datos Personales para la Rama Judicial debe ser realizada de acuerdo con lo establecido en el procedimiento del SGSI “[Procedimiento Informe de Revisión por la Alta Dirección](https://etbcsj.sharepoint.com/teams/Proyecto166-2021SGSI/Documentos%20compartidos/General/SGSI/02%20-%20Etapa%20de%20Ejecución/06%20-%20DOCUMENTOS%20REVISIÓN/Estructura%20ISO%2027001%20V2/4.%20Verificar%20-%20Numeral%209/SGSI%20-%20Procedimiento%20Informe%20de%20%20Revisión%20por%20Alta%20Dirección.docx)”.

1. MEJORA

La Rama Judicial debe propender por la mejora continua del Sistema de Gestión de Seguridad de la Información, Ciberseguridad y Protección de Datos Personales, mediante la verificación del cumplimiento de la política del sistema, los objetivos del sistema, resultados de auditorías y las revisiones por parte de la dirección.

* 1. No conformidades y Acción Correctiva

La Rama Judicial, se compromete a reaccionar frente a las no conformidades, evaluándolas y emprendiendo planes de acción correctivos si son necesarios.

* + 1. Identificación de las no Conformidades

Dado que una no conformidad es el incumplimiento de un requisito sea de manera completa o parcial, dichas no conformidades pueden ser detectadas en cualquiera de estas situaciones:

* La no implementación o el incumplimiento de un requisito, reglamento o control establecidos por la Rama Judicial.
* Registro de incidentes, sin la implementación de los controles establecidos para este tipo de eventos.
* Observaciones en las auditorías realizadas a la Seguridad de la Información, Ciberseguridad y Protección de Datos Personales, en la cual se evidenciaron el incumplimiento de los lineamientos establecidos en el Sistema.
* Resultados de medición fuera de los rangos establecidos por el Sistema de Gestión de Seguridad de la Información, Ciberseguridad y Protección de Datos Personales.
* Incumplimiento de los Objetivos establecidos en el sistema por parte de la Rama Judicial.

Las no conformidades identificadas en las auditorías internas o externas al Sistema de Gestión de Seguridad de la Información, Ciberseguridad y Protección de Datos Personales para la Rama Judicial serán gestionadas de acuerdo con el procedimiento establecido en el Sistema Integrado de Gestión de Calidad y Medio Ambiente (SIGCMA) – “[PROCEDIMIENTO DE CONTROL DE SALIDAS NO CONFORME](https://etbcsj.sharepoint.com/teams/Proyecto166-2021SGSI/Documentos%20compartidos/General/SGSI/02%20-%20Etapa%20de%20Ejecución/06%20-%20DOCUMENTOS%20REVISIÓN/Estructura%20ISO%2027001%20V2/5.%20Actuar%20-%20Numeral%2010/PROCEDIMIENTO%20DE%20CONTROL%20DE%20SALIDAS%20NO%20CONFORME%20.pdf)”.

* + 1. Acciones Correctivas

Frente a las no conformidades detectadas, la Rama Judicial emprenderá las siguientes acciones:

* Identificación del alcance e impacto de la no conformidad
* Se debe elaborar un Plan de Acción que cumpla con los siguientes parámetros:
  + Creación de actividades que limiten el impacto de la no conformidad presentada.
  + Definir los responsables, que llevaran a cabo las actividades definidas para la eliminación de la no conformidad.
  + Plazos para la puesta en marcha y revisión de los resultados obtenidos con el plan de acción.
  + Evaluación de la efectividad de las acciones emprendidas para eliminar la no-conformidad.
  + Se debe verificar que las acciones correctivas no generen efectos secundarios en los procesos.

Las acciones correctivas identificadas como resultados de las no conformidades de las auditorías internas o externas al Sistema de Gestión de Seguridad de la Información, Ciberseguridad y Protección de Datos Personales para la Rama Judicial serán gestionadas de acuerdo con el procedimiento establecido en el Sistema Integrado de Gestión de Calidad y Medio Ambiente (SIGCMA) – “[PROCEDIMIENTO DE ACCIONES DE GESTIÓN](https://etbcsj.sharepoint.com/teams/Proyecto166-2021SGSI/Documentos%20compartidos/General/SGSI/02%20-%20Etapa%20de%20Ejecución/06%20-%20DOCUMENTOS%20REVISIÓN/Estructura%20ISO%2027001%20V2/5.%20Actuar%20-%20Numeral%2010/PROCEDIMIENTO%20DE%20ACCIONES%20DE%20GESTION.pdf)”.

* + 1. Prevención de las No Conformidades

Cuando se detecte una situación que pudiera ser causante de no-conformidades dentro del Sistema de Gestión de Seguridad de la Información, Ciberseguridad y Protección de Datos Personales para la Rama Judicial, se plantearán acciones concretas para eliminar esas no-conformidades potenciales, que incluye lo siguiente:

* Análisis de la causa.
* Elaboración del plan de acción, que incluye:
  + Actividades que se emprenderán para la eliminación de la no-conformidad.
  + Responsables de las actividades definidas para la eliminación de la no-conformidad.
  + Plazos para la puesta en marcha y revisión de los resultados obtenidos con el plan de acción.
  + Evaluación de la efectividad de las acciones emprendidas para eliminar la no-conformidad.
    1. Registro de las No Conformidades

Las no-conformidades deberán ser registradas en el formato establecido en el Sistema Integrado Gestión y Control de la Calidad y del Medio Ambiente (SIGCMA) para documentar las Acciones Preventivas y Correctivas. Este formato, servirá como soporte para el seguimiento del tratamiento de la no-conformidad.

* + 1. Resultados de las Acciones Correctivas y Preventivas

El responsable del proceso, luego de detectar la no-conformidad y de planear y tomar las medidas correctivas o preventivas a que hubiere lugar, consigna en el formato destinado para el seguimiento de las acciones preventivas y correctivas, los resultados que se obtuvieron con tales acciones evidenciando la efectividad de las mismas.

* 1. Mejora Continua

Teniendo en cuenta que el Sistema de Gestión de Seguridad de la Información, Ciberseguridad y Protección de Datos Personales, no es estático debido a cambios que se pueden presentar en la organización y a la evolución constante de los riesgos, es indispensable que el sistema de gestión mencionado se encuentre en un proceso constante de mejora continua para garantizar su efectividad.

Con el fin de que el Sistema de Gestión de Seguridad de la Información, Ciberseguridad y Protección de Datos Personales de la Rama Judicial alcance el nivel de madurez deseado será revisado anualmente o cuando se considere necesario, incluyendo políticas, procedimientos, registros entre otros y teniendo en cuenta los siguientes aspectos:

* Cambios en el contexto externo, interno o de los procesos.
* Cambios en los objetivos estratégicos de la Rama Judicial.
* Cambios en el plan estratégico de la Rama Judicial.
* Cambios en la infraestructura tecnológica.
* Cambios en el alcance del Sistema de Gestión de Seguridad de la Información, Ciberseguridad y Protección de Datos Personales de la Rama Judicial.

1. ANEXOS

* 1. [Anexo A. Plan de Gestión de los Interesados](https://etbcsj.sharepoint.com/teams/Proyecto166-2021SGSI/Documentos%20compartidos/General/SGSI/02%20-%20Etapa%20de%20Ejecución/06%20-%20DOCUMENTOS%20REVISIÓN/Estructura%20ISO%2027001%20V2/2.%20Planear%20-%20Numerales%204,%205,%206%20y%207/Anexo%20A.%20Plan%20de%20Gestión%20de%20los%20Interesados.xlsx)

A continuación, se presenta el plan de gestión de interesados en el Sistema de Gestión de Seguridad de la Información, Ciberseguridad y Protección de Datos Personales:

| **Tipo** | **Dimensión** | **Dirección / Corporación / Entidad** | **Parte Interesada** | **Requisito de la parte interesada** | **Compromiso** | | | | | **Poder / Influencia** | **Interés** | **Estrategia** | **Descripción de la Estrategia** |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Desconoce** | **Se Resiste** | **Neutral** | **Apoya** | **Líder** |
| **INTERNAS** | **Rama Judicial** | **Dirección Ejecutiva de Administración Judicial (DEAJ)** | Despacho del DEAJ | Implementación del Sistema de Gestión de Seguridad de la Información acorde con las necesidades de la Rama Judicial. |  |  |  | X |  | A | A | Gestionar de cerca | Información constante sobre el avance del SGSI, victorias tempranas y dificultades a sortear |
| Grupo de Proyectos Especiales de Infraestructura | Implementación del Sistema de Gestión de Seguridad de la Información acorde con las necesidades de la Rama Judicial. |  |  |  | X |  |  | A | Mantener Informado | Entregar informes periódicos sobre el avance del SGSI |
| Grupo de Proyectos Especiales de Tecnología | Implementación del Sistema de Gestión de Seguridad de la Información acorde con las necesidades de la Rama Judicial. |  |  |  |  | X |  | A | Gestionar de cerca | Información constante sobre el avance del SGSI, victorias tempranas y dificultades a sortear |
| Grupo de Proyectos Transversales | Implementación del Sistema de Gestión de Seguridad de la Información acorde con las necesidades de la Rama Judicial. |  |  |  |  |  | A | A | Gestionar de cerca | Información constante sobre el avance del SGSI y presentar piezas de comunicación para su aprobación y despliegue |
| Unidad de Control Interno Disciplinario | Acceso seguro a la información y protección de datos personales. |  |  | X |  |  | B | B | Monitorear por si cambia de categoría | Evaluar el comportamiento, para verificar si el compromiso cambia dando lugar a un cambio en el nivel de poder - influencia e interés. |
| Unidad de Planeación | Acceso seguro a la información y protección de datos personales. |  |  |  | X |  | A | B | Monitorear por si cambia de categoría | Evaluar el comportamiento, para verificar si el compromiso cambia dando lugar a un cambio en el nivel de poder - influencia e interés. |
| Unidad de Recursos Humanos | Políticas para la selección contratación y terminación de contrato. |  |  |  | X |  | A | A | Mantener Informado | Entregar informes periódicos sobre el avance del SGSI y requerimientos de capacitación en seguridad a los servidores judiciales de la Rama |
| Unidad de Presupuesto | Acceso seguro a la información y protección de la integridad de la misma. |  |  |  | X |  | A | A | Mantener Informado | Entregar informes periódicos sobre el avance del SGSI |
| Unidad Informática | Implementación del Sistema de Gestión de Seguridad de la Información acorde con las necesidades de la Rama Judicial. |  | X |  |  |  | A | A | Gestionar de cerca | Información constante sobre el avance del SGSI, victorias tempranas y dificultades a sortear |
| Unidad de Asistencia Legal | Garantizar que el SGSI implementado cumpla con la normativa legal colombiana y buenas prácticas de gestión de información judicial. |  |  |  | X |  | A | A | Mantener Informado | Entregar informes periódicos sobre el avance del SGSI |
| Unidad Administrativa | Acceso seguro a la información y protección de datos personales. |  |  | X |  |  | B | B | Mantener Informado | Entregar informes periódicos sobre el avance del SGSI |
| Unidad de Infraestructura Física | Acceso seguro a la información y protección de datos personales. Alineamiento de controles con las políticas y procedimientos del SGSI. |  |  |  | X |  | B | A | Mantener Informado | Entregar informes periódicos sobre el avance del SGSI |
| Unidad de Compras Púbicas | Acceso seguro a la información y protección de la integridad de la misma. |  |  | X |  |  | A | A | Gestionar de cerca | Información constante sobre el avance del SGSI, victorias tempranas y dificultades a sortear |
| **Consejo Superior de la Judicatura (CSJ)** | Centro de Documentación Judicial (CENDOJ) | Se les garantice: confidencialidad, integridad, disponibilidad de la información de la Rama Judicial y al mismo tiempo proveer flexibilidad para el intercambio de información. La formalización del SGSI surta el procedimiento de la Coordinación Nacional de Calidad. |  |  |  | X |  | A | A | Gestionar de cerca | Información constante sobre el avance del SGSI, victorias tempranas y dificultades a sortear |
| Escuela Judicial "Rodrigo Lara Bonilla" | Se les garantice: confidencialidad, integridad, disponibilidad de la información de la Rama Judicial y al mismo tiempo proveer flexibilidad para el intercambio de información. |  |  |  | D |  | A | A | Gestionar de cerca | Información constante sobre el avance del SGSI, victorias tempranas y dificultades a sortear |
| Oficina de Asesoría para la Seguridad de la Rama Judicial | Se les garantice: confidencialidad, integridad, disponibilidad de la información del área y al mismo tiempo proveer flexibilidad para el intercambio de información. |  |  |  | D |  | A | A | Mantener Informado | Entregar informes periódicos sobre el avance del SGSI |
| Unidad de Administración de la Carrera Judicial | Acceso seguro a la información y protección de datos personales. |  |  |  | D |  | A | A | Mantener Informado | Entregar informes periódicos sobre el avance del SGSI |
| Unidad de Desarrollo y Análisis Estadístico | Se les garantice: confidencialidad, integridad, disponibilidad de la información del área y al mismo tiempo proveer flexibilidad para el intercambio de información |  |  |  | D |  | A | A | Mantener Informado | Entregar informes periódicos sobre el avance del SGSI |
| Unidad de Registro Nacional de Abogados y Auxiliares de la Justicia | Se les garantice: confidencialidad, integridad, disponibilidad de la información del área y al mismo tiempo proveer flexibilidad para el intercambio de información. |  |  |  | D |  | A | A | Gestionar de cerca | Información constante sobre el avance del SGSI, victorias tempranas y dificultades a sortear |
| **Corte Suprema de Justicia** | Secretaría Sala de Gobierno | Acceso seguro a la información y protección de datos personales. |  |  |  | D |  | A | B | Mantener Informado | Entregar informes periódicos sobre el avance del SGSI |
| Secretaría Sala de Casación Civil y Agraria | Acceso seguro a la información y protección de datos personales. |  |  |  | D |  | A | B | Mantener Informado | Entregar informes periódicos sobre el avance del SGSI |
| Secretaria Sala de Casación Laboral | Acceso seguro a la información y protección de datos personales. |  |  |  | D |  | B | B | Mantener Informado | Entregar informes periódicos sobre el avance del SGSI |
| Secretaria Sala de Casación Penal | Acceso seguro a la información y protección de datos personales. |  |  |  | D |  | B | B | Mantener Informado | Entregar informes periódicos sobre el avance del SGSI |
| Secretaria General | Acceso seguro a la información y protección de datos personales. |  |  |  | D |  | B | B | Mantener Informado | Entregar informes periódicos sobre el avance del SGSI |
| Relatoría de Tutelas | Acceso seguro a la información y protección de datos personales. |  |  |  | D |  | A | A | Mantener Informado | Entregar informes periódicos sobre el avance del SGSI |
| Oficina de Sistemas | Implementación del Sistema de Gestión de Seguridad de la Información acorde con las necesidades de la Rama Judicial. |  |  |  |  | X | A | A | Gestionar de cerca | Información constante sobre el avance del SGSI, victorias tempranas y dificultades a sortear |
| Oficina de Prensa | Acceso seguro a la información y protección de datos personales. |  |  |  | D |  | A | A | Gestionar de cerca | Información constante sobre el avance del SGSI, victorias tempranas y dificultades a sortear. Tenerlo de aliado para el despliegue de las campañas de sensibilización en seguridad de la información |
| Coordinación Administrativa | Acceso seguro a la información y protección de datos personales. |  |  |  | D |  | B | B | Mantener Informado | Entregar informes periódicos sobre el avance del SGSI |
| **Consejo de Estado** | Sala Plena Contenciosa | Acceso seguro a la información y protección de datos personales. |  |  |  | D |  | A | B | Mantener Informado | Entregar informes periódicos sobre el avance del SGSI |
| Sala de gobierno | Acceso seguro a la información y protección de datos personales. |  |  |  | D |  | A | A | Mantener Informado | Entregar informes periódicos sobre el avance del SGSI |
| Sala de consulta y servicio civil | Acceso seguro a la información y protección de datos personales. |  |  |  | D |  | B | B | Mantener Informado | Entregar informes periódicos sobre el avance del SGSI |
| Secretaría general | Acceso seguro a la información y protección de datos personales. |  |  |  | D |  | A | A | Mantener Informado | Entregar informes periódicos sobre el avance del SGSI |
| Relatorías | Acceso seguro a la información y protección de datos personales. |  |  |  | D |  | B | B | Mantener Informado | Entregar informes periódicos sobre el avance del SGSI |
| Oficina de sistemas | Implementación del Sistema de Gestión de Seguridad de la Información acorde con las necesidades de la Rama Judicial. |  |  |  |  | X | A | A | Gestionar de cerca | Información constante sobre el avance del SGSI, victorias tempranas y dificultades a sortear |
| Oficina de prensa | Acceso seguro a la información y protección de datos personales. |  |  |  | D |  | A | A | Gestionar de cerca | Información constante sobre el avance del SGSI, victorias tempranas y dificultades a sortear. Tenerlo de aliado para el despliegue de las campañas de sensibilización en seguridad de la información |
| Coordinación Administrativa | Acceso seguro a la información y protección de datos personales. |  |  |  | D |  | A | B | Mantener Informado | Entregar informes periódicos sobre el avance del SGSI |
| **Corte Constitucional** | Sala Plena | Acceso seguro a la información y protección de datos personales. |  |  |  | D |  | A | A | Mantener Informado | Entregar informes periódicos sobre el avance del SGSI |
| Secretaría general | Acceso seguro a la información y protección de datos personales. |  |  |  | D |  | A | B | Mantener Informado | Entregar informes periódicos sobre el avance del SGSI |
| Relatorías | Acceso seguro a la información y protección de datos personales. |  |  |  | D |  | B | B | Mantener Informado | Entregar informes periódicos sobre el avance del SGSI |
| Oficina de sistemas | Implementación del Sistema de Gestión de Seguridad de la Información acorde con las necesidades de la Rama Judicial. |  |  |  |  | X | A | A | Gestionar de cerca | Información constante sobre el avance del SGSI, victorias tempranas y dificultades a sortear |
| Oficina de prensa | Acceso seguro a la información y protección de datos personales. |  |  |  | D |  | A | A | Gestionar de cerca | Información constante sobre el avance del SGSI, victorias tempranas y dificultades a sortear. Tenerlo de aliado para el despliegue de las campañas de sensibilización en seguridad de la información |
| Coordinación Administrativa | Acceso seguro a la información y protección de datos personales. |  |  |  | D |  | A | B | Mantener Informado | Entregar informes periódicos sobre el avance del SGSI |
| **Comisión Nacional de Disciplina Judicial** | Comunicaciones | Acceso seguro a la información y protección de datos personales. |  |  |  | D |  | A | A | Gestionar de cerca | Información constante sobre el avance del SGSI, victorias tempranas y dificultades a sortear. Tenerlo de aliado para el despliegue de las campañas de sensibilización en seguridad de la información |
| Relatoría | Acceso seguro a la información y protección de datos personales. |  |  |  | D |  | A | B | Mantener Informado | Entregar informes periódicos sobre el avance del SGSI |
| Sistemas | Implementación del Sistema de Gestión de Seguridad de la Información acorde con las necesidades de la Rama Judicial. |  |  |  |  | X | A | A | Gestionar de cerca | Información constante sobre el avance del SGSI, victorias tempranas y dificultades a sortear |
| **Seccionales de la Rama Judicial** | Administración y Financiera | Acceso seguro a la información y protección de datos personales. |  |  | X |  |  | B | B | Mantener Informado | Entregar informes periódicos sobre el avance del SGSI |
| Jurídica | Garantizar que el SGSI implementado cumpla con la normativa legal colombiana y buenas prácticas de gestión de información judicial. |  |  |  | D |  | A | A | Mantener Informado | Entregar informes periódicos sobre el avance del SGSI |
| Talento Humano | Políticas para la selección contratación y terminación de contrato. |  |  |  | D |  | A | A | Mantener Informado | Entregar informes periódicos sobre el avance del SGSI y requerimientos de capacitación en seguridad a los servidores judiciales de la Rama |
| Sistemas | Implementación del Sistema de Gestión de Seguridad de la Información acorde con las necesidades de la Rama Judicial. |  |  |  |  | X | A | A | Gestionar de cerca | Información constante sobre el avance del SGSI, victorias tempranas y dificultades a sortear |
| Tribunales | Acceso seguro a la información y protección de datos personales. |  |  |  | D |  | A | A | Gestionar de cerca | Información constante sobre el avance del SGSI, victorias tempranas y dificultades a sortear |
| Juzgados | Acceso seguro a la información y protección de datos personales. |  |  |  | D |  | B | A | Gestionar de cerca | Información constante sobre el avance del SGSI, victorias tempranas y dificultades a sortear |
| **EXTERNAS** | **GOBIERNO** | | Ministerio de Tecnologías de la Información y las Comunicaciones | Dar cumplimiento a las regulaciones expedidas por dicho ente. |  |  |  | X |  | A | A | Mantener satisfecho | Entregar información oportunamente para que puedan realizar sus funciones en los tiempos establecidos |
| Contraloría General de la República | Garantizar el acceso a la información oportunamente, manteniendo la seguridad de la información. |  |  | X |  |  | A | A | Mantener satisfecho | Entregar información oportunamente para que puedan realizar sus funciones en los tiempos establecidos |
| Procuraduría General de la Nación | Garantizar el acceso a la información oportunamente, manteniendo la seguridad de la información. |  |  | X |  |  | A | A | Mantener satisfecho | Entregar información oportunamente para que puedan realizar sus funciones en los tiempos establecidos |
| Fiscalía General de la Nación | Garantizar el acceso y trasparencia a la información oportunamente, manteniendo la seguridad de la información. |  |  | X |  |  | A | A | Mantener satisfecho | Entregar información oportunamente para que puedan realizar sus funciones en los tiempos establecidos |
| Superintendencia de Industria y Comercio | Garantizar el acceso e intercambio de la información oportunamente, manteniendo la seguridad de la información y la protección de datos personales. |  |  | X |  |  | A | A | Mantener satisfecho | Entregar información oportunamente para que puedan realizar sus funciones en los tiempos establecidos |
| Departamento Administrativo de la Función Pública | Garantizar el acceso e intercambio de la información oportunamente, manteniendo la seguridad de la información. |  |  | X |  |  | A | A | Mantener satisfecho | Entregar información oportunamente para que puedan realizar sus funciones en los tiempos establecidos |
| Archivo General de la Nación | Garantizar el acceso e intercambio de la información oportunamente, manteniendo la seguridad de la información. |  |  | X |  |  | A | A | Mantener satisfecho | Entregar información oportunamente para que puedan realizar sus funciones en los tiempos establecidos |
| Contaduría General de la Nación | Garantizar el acceso e intercambio de la información oportunamente, manteniendo la seguridad de la información. |  |  | X |  |  | A | A | Mantener satisfecho | Entregar información oportunamente para que puedan realizar sus funciones en los tiempos establecidos |
| Dirección de Impuestos y Aduanas Nacionales | Garantizar el acceso e intercambio de la información oportunamente, manteniendo la seguridad de la información. |  |  | X |  |  | A | B | Mantener satisfecho | Entregar información oportunamente para que puedan realizar sus funciones en los tiempos establecidos |
| Ministerio de Hacienda y Crédito Público | Garantizar el acceso e intercambio de la información oportunamente, manteniendo la seguridad de la información. |  |  | X |  |  | B | B | Mantener satisfecho | Entregar información oportunamente para que puedan realizar sus funciones en los tiempos establecidos |
| Agencia Nacional de Contratación Pública (Colombia Compra Eficiente) | Garantizar el acceso e intercambio de la información oportunamente, manteniendo la seguridad de la información. |  |  | X |  |  | A | A | Mantener satisfecho | Entregar información oportunamente para que puedan realizar sus funciones en los tiempos establecidos |
| Ministerio de relaciones exteriores | Garantizar el acceso e intercambio de la información oportunamente, manteniendo la seguridad de la información y la protección de datos personales. |  |  | X |  |  | B | A | Mantener satisfecho | Entregar información oportunamente para que puedan realizar sus funciones en los tiempos establecidos |
| **Usuarios del Servicio de Justicia** | | Observatorios de Justicia | Garantizar el acceso e intercambio de la información oportunamente, manteniendo la seguridad de la información y protección de datos personales. |  |  | X |  |  | B | B | Monitorear por si cambia de categoría | Evaluar el comportamiento, para verificar si el compromiso cambia dando lugar a un cambio en el nivel de poder - influencia e interés. |
| Instituciones de Educación Superior | Garantizar el acceso e intercambio de la información oportunamente, manteniendo la seguridad de la información y protección de datos personales. |  |  | X |  |  | B | B | Monitorear por si cambia de categoría | Evaluar el comportamiento, para verificar si el compromiso cambia dando lugar a un cambio en el nivel de poder - influencia e interés. |
| Personas Jurídicas | Garantizar el acceso e intercambio de la información oportunamente, manteniendo la seguridad de la información y protección de datos personales. Garantizar la protección de la información intercambiada en el acceso al servicio de justicia. |  |  | X |  |  | B | A | Monitorear por si cambia de categoría | Evaluar el comportamiento, para verificar si el compromiso cambia dando lugar a un cambio en el nivel de poder - influencia e interés. |
| Estudiantes | Garantizar el acceso e intercambio de la información oportunamente, manteniendo la seguridad de la información y protección de datos personales. |  |  | X |  |  | B | B | Monitorear por si cambia de categoría | Evaluar el comportamiento, para verificar si el compromiso cambia dando lugar a un cambio en el nivel de poder - influencia e interés. |
| Abogados | Garantizar el acceso e intercambio de la información oportunamente, manteniendo la seguridad de la información y protección de datos personales. |  |  | X |  |  | B | A | Monitorear por si cambia de categoría | Evaluar el comportamiento, para verificar si el compromiso cambia dando lugar a un cambio en el nivel de poder - influencia e interés. |
| Ciudadanía | Garantizar el acceso e intercambio de la información oportunamente, manteniendo la seguridad de la información y protección de datos personales. Garantizar la protección de la información intercambiada en el acceso al servicio de Justicia. |  |  | X |  |  | B | B | Monitorear por si cambia de categoría | Evaluar el comportamiento, para verificar si el compromiso cambia dando lugar a un cambio en el nivel de poder - influencia e interés. |

* 1. Anexo B. [Análisis FODA](https://etbcsj.sharepoint.com/teams/Proyecto166-2021SGSI/Documentos%20compartidos/General/SGSI/02%20-%20Etapa%20de%20Ejecución/06%20-%20DOCUMENTOS%20REVISIÓN/Estructura%20ISO%2027001%20V2/2.%20Planear%20-%20Numerales%204,%205,%206%20y%207/MATRIZ%20DOFA.xlsm)
     1. Estrategias Fortalezas - Oportunidades

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | **FORTALEZAS** | **OPORTUNIDADES** |  | **COMBINACIÓN** | **ESTRATEGIA** | |
| 1 | Se cuenta con un procedimiento de formalización de políticas y procedimientos a nivel de la Rama Judicial a través del Sistema Integrado de Gestión de Calidad y Control Ambiental – SIGCMA. | Los recientes lineamientos sobre seguridad y gobierno de datos emitidas por el gobierno nacional y los ajustes en las normas de seguridad (ISO 27002) impulsan a la revisión y atención de los mismos por un equipo de trabajo especializado en seguridad de la información. |  | F1-O1 | FO1 | Formalizar ante la Coordinación Nacional de Calidad todos los productos (metodologías, políticas y procedimientos) del SGSI definido. |
| 2 | La gestión del programa de seguridad de la información y ciberseguridad está a cargo del Grupo de Proyectos Especiales de Tecnología, acogiendo una de las recomendaciones del Banco Mundial. | Los recientes ciberataques a otras entidades mantienen viva la necesidad de contar con el SGSI implementado y formalizado y esquemas de respuesta apropiados. Se tienen experiencias negativas en protección de información en los años anteriores en la Rama Judicial. |  | F2-O5 | FO2 | Promover antes las diferentes instancias la necesidad que el SGSI definido quede bajo la tutela del CSJ como lo recomienda el Banco Mundial. |
| 3 | En el alcance del contrato 166 de 2021 (en ejecución), se incluye la implementación de la oficina de seguridad de la información apalancada por servicios de monitoreo de seguridad de un SOC basado en herramientas de analítica de datos, lo que facilita la implementación del esquema de seguridad adaptativa. | La dinámica de los ataques y amenazas cibernéticas obliga a que la Rama Judicial revise y fortalezca sus esquemas de defensa. Es un buen momento para posicionar los servicios adquiridos por la Rama Judicial en el marco del contrato 166 de 2021. |  | F3-O2 | FO3 | Impulsar rápidamente el procedimiento de gestión de incidentes en la Rama Judicial. Un ciberataque contenido oportunamente eleva la credibilidad y confianza en la Oficina de Seguridad de la Información. Se deben llevar los indicadores de gestión de la oficina de seguridad. |
| 4 | Fue aprobado el Plan de Transformación Digital de la Rama Judicial (2021 - 2025), en el cual se definen los aspectos principales a tener en cuenta en la implementación del Plan de Seguridad de la Información (PESI). | La capacitación de 25 servidores judiciales en SGSI, Ciberseguridad, Continuidad del Negocio, ley 1581 y MSPI lleva a la Rama Judicial a dar los pasos iniciales en conformar un equipo interno especializado en seguridad de la información y con una gran ventaja: conocen la Rama Judicial. |  | F3-O3 | FO3 | Impulsar rápidamente el procedimiento de gestión de incidentes en la Rama Judicial. Un ciberataque contenido oportunamente eleva la credibilidad y confianza en la Oficina de Seguridad de la Información. Se deben llevar los indicadores de gestión de la oficina de seguridad. |
| 5 | El personal de las diferentes dependencias es consciente de la necesidad de contar con el sistema de gestión de la seguridad de la información (SGSI) transversal a la Rama Judicial. | El Plan de Transformación Digital recomienda que la función de Seguridad de la Información dependa de la Presidencia del CSJ a nivel de asesor, para que la implementación del SGSI sea transversal a toda la Rama Judicial. |  | F4-O4 | FO4 | Promover la certificación de los 25 funcionarios seleccionados para recibir formación en mejores prácticas de seguridad de la información. |
| 6 | El alcance del contrato 166 de 2021 (en ejecución), cubre el CSJ, la DEAJ, las Altas Cortes y la Seccional Bogotá para la implementación del SGSI transversal a la Rama Judicial. La Rama Judicial queda dotada con la base de datos de Activos de Información y Riesgos de Seguridad de la Información centralizada en la Oficina de Seguridad de la Información. | El Plan Estratégico de Seguridad de la Información propuesto por el Banco Mundial en el marco del Plan Estratégico de Transformación Digital dimensiono el presupuesto y las necesidades técnicas y humanas para la implementación de la Oficina de Seguridad de la Información a largo plazo. La Rama Judicial conoce la dimensión del proyecto. |  | F4-O6 | FO5 | Adoptar las recomendaciones del Banco Mundial en lo referente al PESI y acelerar su implementación. Formalizar y proteger el presupuesto anual requerido para la implementación y mantenimiento del programa de seguridad de la información, incluyendo las soluciones de seguridad informática necesarias. |
|  |  |  |  | F5-O1 | FO1 | Formalizar ante la Coordinación Nacional de Calidad todos los productos (metodologías, políticas y procedimientos) del SGSI definido. |
|  |  |  |  | F6-01 | FO1 | Formalizar ante la Coordinación Nacional de Calidad todos los productos (metodologías, políticas y procedimientos) del SGSI definido. |

* + 1. Estrategias Fortalezas - Amenazas

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | **FORTALEZAS** | **AMENAZAS** |  | **COMBINACIÓN** | **ESTRATEGIA** | |
| 1 | Se cuenta con un procedimiento de formalización de políticas y procedimientos a nivel de la Rama Judicial a través del Sistema Integrado de Gestión de Calidad y Control Ambiental – SIGCMA. | Aumento de ataques cibernéticos en el sector público. Si se materializa un ataque a la Rama Judicial, la reputación de la Oficina de Seguridad puede quedar comprometida. |  | F1-A1 | FA1 | Formalizar ante la Coordinación Nacional de Calidad todos los productos (metodologías, políticas y procedimientos) del SGSI definido. |
| 2 | La gestión del programa de seguridad de la información y ciberseguridad está a cargo del Grupo de Proyectos Especiales de Tecnología, acogiendo una de las recomendaciones del Banco Mundial. | Modificación de prioridades por disposiciones del Gobierno, pueden derivar en cambio de planes y destinación de recursos a otras iniciativas. |  | F2-A3 | FA2 | Control de costos en los proyectos del PETD y protección de los recursos destinados al PESI |
| 3 | En el alcance del contrato 166 de 2021 (en ejecución), se incluye la implementación de la oficina de seguridad de la información apalancada por servicios de monitoreo de seguridad de un SOC basado en herramientas de analítica de datos, lo que facilita la implementación del esquema de seguridad adaptativa. | Sobrecostos o identificación de nuevas necesidades en otros proyectos estratégicos del PETD pueden impactar la asignación de recursos al Plan Estratégico de Seguridad de la Información (PESI). |  | F3-A1 | FA3 | Impulsar rápidamente el procedimiento de gestión de incidentes en la Rama Judicial. Un ciberataque contenido eleva la credibilidad y confianza en la Oficina de Seguridad de la Información |
| 4 | Fue aprobado el Plan de Transformación Digital de la Rama Judicial (2021 - 2025), en el cual se definen los aspectos principales a tener en cuenta en la implementación del Plan de Seguridad de la Información (PESI). | Finalización del contrato 166 de 2021 en la fecha prevista y abandono del SGSI en vigencias futuras. |  | F4-A2 | FA4 | Definir los productos esenciales del PESI y que no deben ser objeto de recorte o retiro del plan y acelerar su implementación |
| 5 | El personal de las diferentes dependencias es consciente de la necesidad de contar con el sistema de gestión de la seguridad de la información (SGSI) transversal a la Rama Judicial. | Se finalice la suscripción de las herramientas de seguridad informáticas adquiridas bajo el contrato 166 de 2021 y no se renueven. |  | F4-A5 | FA4 | Definir los productos esenciales del PESI y que no deben ser objeto de recorte o retiro del plan y acelerar su implementación |
| 6 | El alcance del contrato 166 de 2021 (en ejecución), cubre el CSJ, la DEAJ, las Altas Cortes y la Seccional Bogotá para la implementación del SGSI transversal a la Rama Judicial. La Rama Judicial queda dotada con la base de datos de Activos de Información y Riesgos de Seguridad de la Información centralizada en la Oficina de Seguridad de la Información. |  |  | F5-A4 | FA5 | Desplegar el plan de gestión de cambio y sensibilización en seguridad de la información a la Alta Dirección de las diferentes corporaciones. |
|  |  |  |  | F6-A1 | FA6 | Completar el inventario de activos de información y riesgos de seguridad de la información en todas las dependencias de la Rama Judicial. Un inventario actualizado facilita la identificación de riesgos y la adopción de políticas y controles de seguridad sobre activos de información críticos |

* + 1. Estrategias Debilidades - Amenazas

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | **DEBILIDADES** | **AMENAZAS** |  | **COMBINACIÓN** | **ESTRATEGIA** | |
| 1 | La documentación de los procesos (caracterización) de las corporaciones de la Rama Judicial tiene diferentes niveles de madurez. | Aumento de ataques cibernéticos en el sector público. Si se materializa un ataque a la Rama Judicial, la reputación de la Oficina de Seguridad puede quedar comprometida. |  | D1 - A1 | DA1 | Formalizar ante la Coordinación Nacional de Calidad todos los productos (metodologías, políticas y procedimientos) del SGSI definido. Activar protocolos de acuerdo con mejores prácticas, así no estén formalizados en la Rama Judicial |
| 2 | El proceso de aprobación (formalización) del SGSI exige un trámite interno diferente en cada Corporación (diferentes tiempos y prioridades del SGSI). Es posible que el SGSI no se alcance a formalizar dentro del periodo de tiempo establecido para el contrato 166 de 2021. | Modificación de prioridades por disposiciones del Gobierno, pueden derivar en cambio de planes y destinación de recursos a otras iniciativas. |  | D1 - A2 | DA5 | Desplegar el plan de gestión de cambio y sensibilización en seguridad de la información a la Alta Dirección de las diferentes corporaciones. |
| 3 | No se cuenta con un registro documentado del seguimiento al cumplimiento de las políticas de seguridad aprobadas en 2014 y por ende no se cuenta con indicadores de la eficacia de la política (no hay historia). | Sobrecostos o identificación de nuevas necesidades en otros proyectos estratégicos del PETD pueden impactar la asignación de recursos al Plan Estratégico de Seguridad de la Información (PESI). |  | D2 - A1 | DA1 | Formalizar ante la Coordinación Nacional de Calidad todos los productos (metodologías, políticas y procedimientos) del SGSI definido. Activar protocolos de acuerdo con mejores prácticas, así no estén formalizados en la Rama Judicial |
| 4 | Carencia de un equipo interno especializado en seguridad de la información que dé respuesta oportuna a los hallazgos de diferentes auditorias. En 2022 se dio inicio a la revisión de informes de auditoría correspondientes al periodo 2018 – 2021. | Finalización del contrato 166 de 2021 en la fecha prevista y abandono del SGSI en vigencias futuras. |  | D4 - A1 | DA2 | Iniciar la transición de la Oficina de Seguridad de la Información con el personal interno que se logre certificar en 2022 y mantener su funcionamiento mediante esquema mixto (parte personal de un tercero, parte personal interno de la Rama Judicial) |
| 5 | La Rama Judicial se define como una entidad diferente y particular que requiere personalización especial de las reglamentaciones de riesgos, seguridad, continuidad, otros. Esto puede generar devolución de productos por no tener la Rama un marco de referencia inicialmente aprobado. | Se finalice la suscripción de las herramientas de seguridad informáticas adquiridas bajo el contrato 166 de 2021 y no se renueven. |  | D5 - A1 | DA1 | Formalizar ante la Coordinación Nacional de Calidad todos los productos (metodologías, políticas y procedimientos) del SGSI definido. Activar protocolos de acuerdo con mejores prácticas, así no estén formalizados en la Rama Judicial |
| 6 | La autonomía de las corporaciones que conforman la Rama Judicial para el desarrollo de sus actividades, puede llevar a que la implementación del SGSI tenga diferentes niveles de prioridad en cada entidad. |  |  | D6 - A4 | DA3 | Extender el alcance del contrato 166 de 2021 |
| 7 | Durante el proyecto se han detectado problemas de competencia y/o colaboración entre diferentes unidades de la Rama Judicial. Los productos del contrato 166 de 2021 podrían no ser aceptados o relegados por diferentes unidades de la Rama Judicial (Resistencia al cambio). |  |  | D4-A5 | DA3 | Extender el alcance del contrato 166 de 2021 |
|  |  |  |  | D7-A3 | DA4 | Control de costos en los proyectos del PETD y protección de los recursos destinados al PESI |

* + 1. Estrategias Debilidades - Oportunidades

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | **DEBILIDADES** | **OPORTUNIDADES** |  | **COMBINACIÓN** | **ESTRATEGIA** | |
| 1 | La documentación de los procesos (caracterización) de las corporaciones de la Rama Judicial tiene diferentes niveles de madurez. | Los recientes lineamientos sobre seguridad y gobierno de datos emitidas por el gobierno nacional y los ajustes en las normas de seguridad (ISO 27002) impulsan a la revisión y atención de los mismos por un equipo de trabajo especializado en seguridad de la información. |  | D1 - O1 | DO1 | Establecer políticas de seguridad de la información, teniendo en cuenta los lineamientos y recomendaciones establecidas en el MSPI definido por el MINTIC y mejores prácticas de Seguridad de la Información (SGSI) |
| 2 | El proceso de aprobación (formalización) del SGSI exige un trámite interno diferente en cada Corporación (diferentes tiempos y prioridades del SGSI). Es posible que el SGSI no se alcance a formalizar dentro del periodo de tiempo establecido para el contrato 166 de 2021. | Los recientes ciberataques a otras entidades mantienen viva la necesidad de contar con el SGSI implementado y formalizado y esquemas de respuesta apropiados. Se tienen experiencias negativas en protección de información en los años anteriores en la Rama Judicial. |  | D1 - O2 | DO2 | Impulsar rápidamente el procedimiento de gestión de incidentes en la Rama Judicial. Un ciberataque contenido eleva la credibilidad y confianza en la Oficina de Seguridad de la Información |
| 3 | No se cuenta con un registro documentado del seguimiento al cumplimiento de las políticas de seguridad aprobadas en 2014 y por ende no se cuenta con indicadores de la eficacia de la política (no hay historia). | La dinámica de los ataques y amenazas cibernéticas obliga a que la Rama Judicial revise y fortalezca sus esquemas de defensa. Es un buen momento para posicionar los servicios adquiridos por la Rama Judicial en el marco del contrato 166 de 2021. |  | D1 - O3 | DO2 | Impulsar rápidamente el procedimiento de gestión de incidentes en la Rama Judicial. Un ciberataque contenido eleva la credibilidad y confianza en la Oficina de Seguridad de la Información |
| 4 | Carencia de un equipo interno especializado en seguridad de la información que dé respuesta oportuna a los hallazgos de diferentes auditorias. En 2022 se dio inicio a la revisión de informes de auditoría correspondientes al periodo 2018 – 2021. | La capacitación de 25 servidores judiciales en SGSI, Ciberseguridad, Continuidad del Negocio, ley 1581 y MSPI lleva a la Rama Judicial a dar los pasos iniciales en conformar un equipo interno especializado en seguridad de la información y con una gran ventaja: conocen la Rama Judicial. |  | D1 - O5 | DO3 | Promover antes las diferentes instancias la necesidad que el SGSI definido quede bajo la tutela del CSJ como lo recomienda el Banco Mundial. |
| 5 | La Rama Judicial se define como una entidad diferente y particular que requiere personalización especial de las reglamentaciones de riesgos, seguridad, continuidad, otros. Esto puede generar devolución de productos por no tener la Rama un marco de referencia inicialmente aprobado. | El Plan de Transformación Digital recomienda que la función de Seguridad de la Información dependa de la Presidencia del CSJ a nivel de asesor, para que la implementación del SGSI sea transversal a toda la Rama Judicial. |  | D2 - O4 | DO4 | Promover la capacitación y certificación de los 25 funcionarios seleccionados para recibir capacitación especializada en SGSI, MSPI, Ciberseguridad y Ley de Protección de Datos. |
| 6 | La autonomía de las corporaciones que conforman la Rama Judicial para el desarrollo de sus actividades, puede llevar a que la implementación del SGSI tenga diferentes niveles de prioridad en cada entidad. | El Plan Estratégico de Seguridad de la Información propuesto por el Banco Mundial en el marco del Plan Estratégico de Transformación Digital dimensiono el presupuesto y las necesidades técnicas y humanas para la implementación de la Oficina de Seguridad de la Información a largo plazo. La Rama Judicial conoce la dimensión del proyecto. |  | D4 - O4 | DO4 | Promover la certificación de los 25 funcionarios seleccionados para recibir formación en mejores prácticas de seguridad de la información. |
| 7 | Durante el proyecto se han detectado problemas de competencia y/o colaboración entre diferentes unidades de la Rama Judicial. Los productos del contrato 166 de 2021 podrían no ser aceptados o relegados por diferentes unidades de la Rama Judicial (Resistencia al cambio). |  |  | D5 - O4 | DO4 | Promover la certificación de los 25 funcionarios seleccionados para recibir formación en mejores prácticas de seguridad de la información. |
|  |  |  |  | D6 - O4 | DO4 | Promover la certificación de los 25 funcionarios seleccionados para recibir formación en mejores prácticas de seguridad de la información. |
|  |  |  |  | D7 - O4 | DO4 | Promover la certificación de los 25 funcionarios seleccionados para recibir formación en mejores prácticas de seguridad de la información. |

* + 1. Resultados análisis FODA

|  |  |  |
| --- | --- | --- |
|  | **FORTALEZAS** | **DEBILIDADES** |
| **Resultados análisis FODA para el Sistema de Gestión de Seguridad de la Información, Ciberseguridad y Protección de Datos Personales de la Rama Judicial** | Se cuenta con un procedimiento de formalización de políticas y procedimientos a nivel de la Rama Judicial a través del Sistema Integrado de Gestión de Calidad y Control Ambiental - SIGCMA | La documentación de los procesos (caracterización) de las corporaciones de la Rama Judicial tiene diferentes niveles de madurez |
| La gestión del programa de seguridad de la información y ciberseguridad está a cargo del Grupo de Proyectos Especiales de Tecnología, acogiendo una de las recomendaciones del Banco Mundial | El proceso de aprobación (formalización) del SGSI exige un trámite interno diferente en cada Corporación (diferentes tiempos y prioridades del SGSI). Es posible que el SGSI no se alcance a formalizar dentro del periodo de tiempo establecido para el contrato 166 de 2021 |
| En el alcance del contrato 166 de 2021 (en ejecución), se incluye la implementación de la oficina de seguridad de la información apalancada por servicios de monitoreo de seguridad de un SOC basado en herramientas de analítica de datos, lo que facilita la implementación del esquema de seguridad adaptativa. | No se cuenta con un registro documentado del seguimiento al cumplimiento de las políticas de seguridad aprobadas en 2014 y por ende no se cuenta con indicadores de la eficacia de la política (no hay historia) |
| Fue aprobado el Plan de Transformación Digital de la Rama Judicial (2021 - 2025), en el cual se definen los aspectos principales a tener en cuenta en la implementación del Plan de Seguridad de la Información (PESI) | Carencia de un equipo interno especializado en seguridad de la información que dé respuesta oportuna a los hallazgos de diferentes auditorias. En 2022 se dio inicio a la revisión de informes de auditoria correspondientes al periodo 2018 - 2021 |
| El personal de las diferentes dependencias es consciente de la necesidad de contar con el sistema de gestión de la seguridad de la información (SGSI) transversal a la Rama Judicial | La Rama Judicial se define como una entidad diferente y particular que requiere personalización especial de las reglamentaciones de riesgos, seguridad, continuidad, otros. Esto puede generar devolución de productos por no tener la Rama un marco de referencia inicialmente aprobado. |
| El alcance del contrato 166 de 2021 (en ejecución), cubre el CSJ, la DEAJ, las Altas Cortes y la Seccional Bogotá para la implementación del SGSI transversal a la Rama Judicial. La Rama Judicial queda dotada con la base de datos de Activos de Información y Riesgos de Seguridad de la Información centralizada en la Oficina de Seguridad de la Información. | La autonomía de las corporaciones que conforman la Rama Judicial para el desarrollo de sus actividades puede llevar a que la implementación del SGSI tenga diferentes niveles de prioridad en cada entidad. |
|  | Durante el proyecto se han detectado problemas de competencia y/o colaboración entre diferentes unidades de la Rama Judicial. Los productos del contrato 166 de 2021 podrían no ser aceptados o relegados por diferentes unidades de la Rama Judicial (Resistencia al cambio) |
| **OPORTUNIDADES** | **ESTRATEGIAS FO** | **ESTRATEGIAS DO** |
| Los recientes lineamientos sobre seguridad y gobierno de datos emitidas por el gobierno nacional y los ajustes en las normas de seguridad (ISO 27002) impulsan a la revisión y atención de los mismos por un equipo de trabajo especializado en seguridad de la información. | - Formalizar ante la Coordinación Nacional de Calidad todos los productos (metodologías, políticas y procedimientos) del SGSI definido. - Promover antes las diferentes instancias la necesidad que el SGSI definido quede bajo la tutela del DEAJ o el CSJ como lo recomienda el Banco Mundial. - Impulsar rápidamente el procedimiento de gestión de incidentes en la Rama Judicial. Un ciberataque contenido eleva la credibilidad y confianza en la Oficina de Seguridad de la Información - Promover la capacitación y certificación de los 25 funcionarios seleccionados para recibir capacitación especializada en SGSI, MSPI, Ciberseguridad y Ley de Protección de Datos. - Adoptar las recomendaciones del Banco Mundial en lo referente al PESI y acelerar su implementación | - Establecer políticas de seguridad de la información, teniendo en cuenta los lineamientos y recomendaciones establecidas en el MSPI definido por el MINTIC - Impulsar rápidamente el procedimiento de gestión de incidentes en la Rama Judicial. Un ciberataque contenido eleva la credibilidad y confianza en la Oficina de Seguridad de la Información - Promover antes las diferentes instancias la necesidad que el SGSI definido quede bajo la tutela del DEAJ o el CSJ como lo recomienda el Banco Mundial. - Promover la capacitación y certificación de los 25 funcionarios seleccionados para recibir capacitación especializada en SGSI, MSPI, Ciberseguridad y Ley de Protección de Datos. |
| Los recientes ciberataques a otras entidades mantienen viva la necesidad de contar con el SGSI implementado y formalizado y esquemas de respuesta apropiados. Se tienen experiencias negativas en protección de información en los años anteriores en la Rama Judicial |
| La dinámica de los ataques y amenazas cibernéticas obliga a que la Rama Judicial revise y fortalezca sus esquemas de defensa. Es un buen momento para posicionar los servicios adquiridos por la Rama Judicial en el marco del contrato 166 de 2021 |
| La capacitación de 25 servidores judiciales en SGSI, Ciberseguridad, Continuidad del Negocio, ley 1581 y MSPI lleva a la Rama Judicial a dar los pasos iniciales en conformar un equipo interno especializado en seguridad de la información y con una gran ventaja: conocen la Rama Judicial. |
| El Plan de Transformación Digital recomienda que la función de Seguridad de la Información dependa de la Presidencia del CSJ a nivel de asesor, para que la implementación del SGSI sea transversal a toda la Rama Judicial |
| El Plan Estratégico de Seguridad de la Información propuesto por el Banco Mundial en el marco del Plan Estratégico de Transformación Digital dimensiono el presupuesto y las necesidades técnicas y humanas para la implementación de la Oficina de Seguridad de la Información a largo plazo. La Rama Judicial conoce la dimensión del proyecto |
| **AMENAZAS** | **ESTRATEGIAS FA** | **ESTRATEGIAS DA** |
| Aumento de ataques cibernéticos en el sector público. Si se materializa un ataque a la Rama Judicial, la reputación de la Oficina de Seguridad puede quedar comprometida. | - Formalizar ante la Coordinación Nacional de Calidad todos los productos (metodologías, políticas y procedimientos) del SGSI definido. - Impulsar rápidamente el procedimiento de gestión de incidentes en la Rama Judicial. Un ciberataque contenido eleva la credibilidad y confianza en la Oficina de Seguridad de la Información - Desplegar el plan de gestión de cambio y sensibilización en seguridad de la información en todas las dependencias de la Rama Judicial.  - Completar el inventario de activos de información y riesgos de seguridad de la información en todas las dependencias de la Rama Judicial. | - Formalizar ante la Coordinación Nacional de Calidad todos los productos (metodologías, políticas y procedimientos) del SGSI definido. - Iniciar la transición de la Oficina de Seguridad de la Información con el personal interno que se logre certificar en 2022 y mantener su funcionamiento mediante esquema mixto (parte personal de un tercero, parte personal interno de la Rama Judicial) - Extender el alcance del contrato 166 de 2021 - Control de costos en los proyectos del PETD y protección de los recursos destinados al PESI - Desplegar el plan de gestión de cambio y sensibilización en seguridad de la información a la Alta Dirección de las diferentes corporaciones. |
| Modificación de prioridades por disposiciones del Gobierno, pueden derivar en cambio de planes y destinación de recursos a otras iniciativas |
| Sobrecostos o identificación de nuevas necesidades en otros proyectos estratégicos del PETD pueden impactar la asignación de recursos al Plan Estratégico de Seguridad de la Información (PESI) |
| Finalización del contrato 166 de 2021 en la fecha prevista y abandono del SGSI en vigencias futuras |
| Se finalice la suscripción de las herramientas de seguridad informáticas adquiridas bajo el contrato 166 de 2021 y no se renueven |

* 1. Anexo C. [Plan de mejoramiento](https://etbcsj.sharepoint.com/teams/Proyecto166-2021SGSI/Documentos%20compartidos/General/SGSI/02%20-%20Etapa%20de%20Ejecución/06%20-%20DOCUMENTOS%20REVISIÓN/Estructura%20ISO%2027001%20V2/5.%20Actuar%20-%20Numeral%2010/CSJ%20-%20Plan%20de%20mejoramiento%20del%20SGSI.docx)

A continuación, se presenta el plan de mejoramiento para el Sistema de Gestión de Seguridad de la Información, Ciberseguridad y Protección de Datos Personales de la Rama Judicial:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | **Año 2022** |  |  | **Año 2023** |
| **Estratégico** | Formalizar ante la Coordinación Nacional de Calidad todos los productos (metodologías, políticas y procedimientos) del SGSI definido. (FODA). |  | **Estratégico** | Garantizar presupuesto para el SGSI. |
| Promover antes las diferentes instancias la necesidad que el SGSI definido quede bajo la tutela del DEAJ o el CSJ como lo recomienda el Banco Mundial. (FODA). |  | Revisar los Resultados por la Dirección. |
| Impulsar rápidamente el procedimiento de gestión de incidentes en la Rama Judicial. (FODA). |  | Revisar los resultados de Evaluación de Nivel de Madurez del SGSI. |
| Promover la capacitación y certificación de los 25 funcionarios seleccionados para recibir capacitación especializada en SGSI, MSPI, Ciberseguridad y Ley de Protección de Datos. (FODA). |  | ***Actividades de mantenimiento*** |
| Desplegar el plan de gestión de cambio y sensibilización en seguridad de la información en todas las dependencias de la Rama Judicial. (FODA). |  | Revisión y actualización de políticas, objetivos y métricas del SGSI. |
| Adoptar las recomendaciones del Banco Mundial en lo referente al PESI y acelerar su implementación. (FODA). |  | Revisión y actualización de requisitos de las partes interesadas del SGSI. |
| Aprobar el Alcance del SGSI de la Rama Judicial. |  | Definir programa de formación, sensibilización y concienciación del SGSI (2023). |
| Aprobar la política general y los objetivos del SGSI. |  | Evaluar Acciones Correctivas originadas en las auditorías internas al SGSI |
| Aprobar la Metodología de Gestión de Activos y Riesgos de Seguridad de la Información. |  | Identificar opciones de mejora al SGSI. |
| Aprobar los niveles de aceptación de riesgos. |  |  |
| Aprobar la Declaración de Aplicabilidad -SOA. |  |  |
| Autorizar los Roles y Responsabilidades definidos para el SGSI de la Rama Judicial. |  |  |
| Conformar el Comité de Seguridad de la Información. |  |  |
| Aprobar los indicadores de gestión del SGSI. |  |  |
| Establecer políticas de seguridad de la información, teniendo en cuenta los lineamientos y recomendaciones establecidas en el MSPI definido por el MINTIC. (FODA). |  |  |
| Aprobar políticas específicas de seguridad de la información con base en las mejores prácticas Anexo A ISO27001 y MSPI. |  |  |
| Iniciar la transición de la Oficina de Seguridad de la Información con el personal interno que se logre certificar en 2022 y mantener su funcionamiento mediante esquema mixto (parte personal de un tercero, parte personal interno de la Rama Judicial). (FODA). |  |  |
| Definir el Portafolio de Proyectos del SGSI. |  |  |
| Extender el alcance del contrato 166 de 2021. |  |  |
|  |  |  |  |  |
| **Táctico** | Completar el inventario de activos de información y riesgos de seguridad de la información en todas las dependencias de la Rama Judicial. |  | **Táctico** | Evaluar el nivel de Madurez del SGSI. |
| Aprobar los riesgos residuales de seguridad de la información. |  | Aprobar Riesgos Residuales MSPI. |
| Aprobar los planes de tratamiento para los riesgos residuales de seguridad de la información no tolerables por la Rama Judicial. |  | ***Actividades de mantenimiento*** |
| Ejecutar el programa de formación, sensibilización y concienciación del SGSI. |  | Análisis y evaluación de riesgos de seguridad de la información (2023). |
| Realizar el Registro Nacional de Bases de Datos. |  | Definir planes de tratamiento para los riesgos residuales de seguridad de la información no tolerables por la Rama Judicial. |
| Definir Programación de Auditorias al MSPI |  | Actualización del Registro Nacional de Bases de Datos. |
|  |  | Realizar campañas de sensibilización y concienciación de MSPI. |
|  |  | Planificación de auditoría Interna/ Externa. |
|  |  |  |  |  |
| **Operativo** | Implementar y monitorear la eficacia de los planes de tratamiento. |  | **Operativo** | ***Actividades de mantenimiento*** |
| Analizar vulnerabilidades y hacer seguimiento a la remediación. |  | Actualizar el inventario de Activos de seguridad de la información. |
| Implementar procedimiento para la Gestión de Incidentes de seguridad de la información. |  | Implementar y monitorear los planes de tratamiento para los riesgos residuales definidos. |
| Reporte de eventos e incidentes de seguridad de la información. |  | Analizar vulnerabilidades y hacer seguimiento a la remediación. |
| Medir los indicadores definidos del SGSI. |  | Reporte de eventos e incidentes de seguridad de la información. |
| Realizar auditorías al SGSI. |  | Medir los indicadores definidos del SGSI. |
|  |  | Realizar Auditorías al SGSI. |

* 1. Anexo D. Perfiles del SGSI

A continuación, se presentan los perfiles profesionales del personal de la Oficina de Seguridad de la Información:

**Director de la Oficina de Seguridad de la Información**

El director de la Oficina de Seguridad de la Información es el encargado de alinear los objetivos y las iniciativas de seguridad de la información y ciberseguridad con los objetivos estratégicos y proyectos de la Rama Judicial. Debe tener el siguiente perfil profesional:

* Profesional en Ingeniería de Sistemas o carreras afines.
* Postgrado en Seguridad de la Información, Seguridad Informática, Ciberseguridad o Gestión de riesgos.
* Experiencia profesional general de más de 15 años.
* Mínimo 10 años de experiencia en gestión de riesgos y seguridad de la información.
* Experiencia y conocimiento en temas asociados a la administración de justicia.
* Deseable que ostente alguna certificación como CISSP, CISM, CISA.

**Oficial de Seguridad de la Información**

El Oficial de Seguridad de la Información debe tener el siguiente perfil profesional:

* Profesional en Ingeniería de Sistemas o carreras afines.
* Especializado en Seguridad de la información, Seguridad informática o ciberseguridad.
* Experiencia profesional general de más de 8 años.
* Mínimo 5 años de experiencia en seguridad de la información.
* Deseable que ostente alguna certificación como CISSP, CISM, CISA, Implementador Líder ISO 27001:2013, Líder de Ciberseguridad o CBCP.

**Coordinador de Seguridad de la Información**

El Coordinador de Seguridad de la Información debe tener el siguiente perfil profesional:

* Profesional en Ingeniería de Sistemas o carreras afines.
* Especializado en Seguridad de la información, Seguridad informática o Gestión de riesgos.
* Experiencia profesional general de más de 6 años.
* Mínimo 5 años de experiencia en seguridad de la información.
* Deseable que ostente alguna certificación como CISM, CISA, Implementador Líder ISO 27001:2013.

**Coordinador de Ciberseguridad**

El Coordinador de Ciberseguridad debe tener el siguiente perfil profesional:

* Profesional en Ingeniería de Sistemas o carreras afines.
* Especializado en Seguridad de la información, Seguridad informática o ciberseguridad.
* Experiencia profesional general de más de 6 años.
* Mínimo 5 años de experiencia en seguridad de la información.
* Deseable que ostente alguna certificación como CISSP, CISM, CISA, Implementador Líder ISO 27001:2013, Líder de Ciberseguridad.

**Analistas de Seguridad y Analistas de Ciberseguridad**

Los Analistas de Seguridad y Analistas de Ciberseguridad, deben tener el siguiente perfil profesional:

* Profesional en Ingeniería de Sistemas o carreras afines.
* Experiencia profesional general de más de 5 años.
* Mínimo 3 años de experiencia en seguridad de la información.
* Deseable que ostenten alguna certificación como Implementadores ISO 27001:2013, Implementadores ISO 22301:2019, Líderes de Ciberseguridad.

**Coordinador de Protección de Datos Personales**

El Coordinador de Protección de Datos Personales debe tener el siguiente perfil profesional:

* Profesional titulado en derecho.
* Experiencia profesional general de mínimo 5 años de experiencia.
* Experiencia laboral y conocimiento de la Ley de Protección de Datos Personales, responsabilidad demostrada y cumplimiento.
* Conocimientos en seguridad de la información, Modelo de Seguridad Privacidad de la Información del MinTIC y gestión de riesgos de seguridad de la información.
* Deseable certificación ISO 27001:2013.

1. Fuente: Adaptación de la Guía del PMBOK® 4ta edición [↑](#footnote-ref-2)
2. Información extraída de la Metodología de Gestión de Activos y Riesgos de Seguridad de la Información, numeral 4.4.3 “Análisis y valoración del riesgo residual”. [↑](#footnote-ref-3)
3. Información extraída de la Metodología de Gestión de Activos y Riesgos de Seguridad de la Información, numeral 4.5 “Riesgo Deseado”. [↑](#footnote-ref-4)