Tel.: 2295-3386 Fax: 2257-0412 Correo: tecnologia-info@poder-judicial.go.cr

Política	PL-SGSI-001	**Fecha actualización:**	26/10/2019	**Página #:**	1 de 7
Título:	Política de Seguridad de la Información				

Política de Seguridad de la Información

1.0 PROPÓSITO

El propósito de esta política de primer nivel es regular las actividades pertinentes a la seguridad de la información y su sistema de gestión (SGSI), mediante el establecimiento de objetivos, principios y reglas básicas que permitan al Poder Judicial alcanzar sus objetivos estratégicos y cumplir con los requisitos legales y regulatorios aplicables.

2.0 ALCANCE

Esta política aplica para todo el Poder Judicial, todas las personas que laboran para él y terceras partes de cualquier índole que acceden y utilizan los activos de información del Poder Judicial.

3.0 TÉRMINOS Y DEFINICIONES

Para un mejor entendimiento de esta política, se deben tener en cuenta los siguientes términos y definiciones:

- Administración Superior: Está constituida por la Corte Plena y el Consejo Superior del Poder Judicial.
- Amenaza: Es cualquier persona, gesto o acción que se anticipa a la intención de causar algún tipo de daño.
- Confidencialidad: Propiedad de que la información no esté disponible o sea divulgada a individuos, entidades o procesos no autorizados.
- Disponibilidad: Propiedad de ser accesible y utilizable a petición de una entidad autorizada.
- Integridad: Propiedad de exactitud y completitud.
- Política: Representan las expectativas y deseos de la Administración Superior. Son consideradas como obligatorias y normalmente son de alto nivel, por lo que no cita detalles.
- Persona usuaria: Persona tanto interna como externa al Poder Judicial que utiliza cualquier servicio o bien que tenga acceso a los diferentes recursos tecnológicos del Poder Judicial.

Tel.: 2295-3386 Fax: 2257-0412 Correo: tecnologia-info@poder-judicial.go.cr

- Riesgo: Es la probabilidad de que una amenaza se materialice y cause un daño o perjuicio.
- Seguridad de la información: Preservación de la confidencialidad, integridad y disponibilidad de la información en cualquiera de los medios en los que se presente, sean impresos, electrónicos, telemáticos y otras fuentes.
- SGSI: Es un Sistema de Gestión de la Seguridad de la Información, que consiste en una serie de actividades de gestión que deben realizarse mediante procesos sistemáticos, documentados y conocidos por una organización o entidad.
- Recursos tecnológicos: Son los componentes o dispositivos tanto de hardware (recursos tangibles como computadoras, impresoras, equipo de comunicaciones, etc.), como de software (recursos intangibles como programas o sistemas informáticos), que permiten a una persona interactuar directa o indirectamente con la información; ya sea leerla, copiarla, moverla, transmitirla, escucharla o visualizarla, para satisfacer una necesidad.

4.0 OBJETIVOS DE SEGURIDAD DE LA INFORMACIÓN

Mediante la seguridad de la información y la implementación del SGSI, el Poder Judicial pretende lograr los siguientes objetivos:

a. Conocer y tratar los riesgos estratégicos y operacionales de seguridad de la información y continuidad del negocio para que se mantengan en un nivel aceptable para el Poder Judicial, incluyendo aquellos relacionados con el cumplimiento de las legislaciones y regulaciones aplicables.

b. Proveer servicios tecnológicos institucionales y de atención al público seguros, donde se proteja la confidencialidad de los datos de las personas usuarias, la integridad de la información sensible de los procesos judiciales, y se garantice de acuerdo con su nivel de criticidad, que dicha información esté disponible para las personas autorizadas.

c. Contar con personas capacitadas y comprometidas con el cumplimiento de las políticas, lineamientos y procedimientos relativos a la seguridad de la información, así como técnicamente preparadas para asegurar que las medidas de protección definidas puedan ser correctamente implementadas y administradas durante todo su ciclo de vida.

Tel.: 2295-3386 Fax: 2257-0412 Correo: tecnologia-info@poder-judicial.go.cr

Política	PL-SGSI-001	**Fecha actualización:**	26/10/2019	**Página #:**	3 de 7
Título:	Política de Seguridad de la Información				

5.0 RESPONSABILIDADES

Con el fin de lograr los objetivos de seguridad de la información y cumplir con los requisitos de esta política se describen las siguientes responsabilidades:

1) Administración Superior

a. Valorar y aprobar las políticas y/o lineamientos generales y específicos en materia de seguridad de la información del Poder Judicial.

b. Procurar los recursos presupuestarios, físicos y recursos humanos que se requieran para la implementación y operación del SGSI, y el cumplimiento de las políticas y/o lineamientos de seguridad institucionales.

c. Valorar y aprobar las estrategias, planes, proyectos, recomendaciones, indicadores y métricas en materia de seguridad de la información, propuestos por las diferentes instancias de coordinación en temas de tecnología de información y comunicaciones en el Poder Judicial.

2) Auditoría Interna

a. Verificar y evaluar el cumplimiento de las políticas y/o lineamientos relacionados con la seguridad de la información.

3) Comisión Gerencial de Tecnologías de la Información y Comunicaciones

a. Promover el desarrollo institucional de la seguridad de la información, para que se haga conforme a un proceso de planificación estratégica que esté alineado con el Plan Estratégico Institucional y el Plan Estratégico de Tecnologías de Información.

b. Proponer políticas y/o lineamientos a la Administración Superior para que constituyan el marco de referencia de seguridad de la información, a partir de las propuestas que le facilite la Dirección de Tecnología de Información y Comunicaciones.

c. Dar seguimiento y apoyo a la seguridad de la información, así como al presupuesto en esta materia.

d. Elevar a la Administración Superior las métricas, indicadores y evaluaciones facilitadas por la Dirección de Tecnología de Información y Comunicaciones, que permitan medir el desempeño de la seguridad de la información en el Poder Judicial y tomar decisiones en relación a su mejora continua.

e. Proponer planes, estrategias y proyectos a la Administración Superior con el fin de promover una cultura de seguridad institucional.

Tel.: 2295-3386 Fax: 2257-0412 Correo: tecnologia-info@poder-judicial.go.cr

Política	PL-SGSI-001	**Fecha actualización:**	26/10/2019	**Página #:**	4 de 7
Título:	Política de Seguridad de la Información				

4) Dirección de Tecnología de Información y Comunicaciones

a. Velar, en conjunto con la Administración Superior, por la implementación y operación del Sistema de Gestión de Seguridad de la Información (SGSI) en su componente tecnológico.

b. Formular las políticas y/o lineamientos generales y específicas en materia tecnológica para la seguridad de la información del Poder Judicial y velar por su cumplimiento.

c. Velar, en conjunto con la Administración Superior, porque todas las personas que laboran para la organización, conozcan y estén comprometidos con las políticas y/o lineamientos de seguridad de la información y las consecuencias de su incumplimiento.

d. Desarrollar e implementar los proyectos tecnológicos en materia de seguridad de la información que hayan sido aprobados por la Administración Superior.

e. Velar por las condiciones físicas y ambientales donde se encuentran instalados los diferentes recursos tecnológicos utilizados para brindar servicios.

f. Velar por la integridad de la información en todos los procesos de implementación de las nuevas aplicaciones, así como en los procesos de mantenimiento de software e infraestructura.

g. Definir los mecanismos que permitan aplicar y verificar el cumplimiento de la seguridad tecnológica, según lo establecido en esta política.

h. Gestionar los proyectos de seguridad informática, y participar en aquellos donde se utilice la tecnología de información como elemento estratégico para el cumplimiento de los objetivos.

i. Detectar, analizar y resolver de forma oportuna los problemas e incidentes de seguridad que se presenten en la plataforma tecnológica.

j. Delegar la implementación de procedimientos y estándares que se desprenden de las políticas y/o lineamientos de seguridad de la información.

k. Proponer estrategias y soluciones específicas para la implantación de los controles necesarios, destinados a cumplir con las políticas y/o lineamientos de seguridad establecidos y la debida solución de las situaciones de riesgo detectadas en el ámbito tecnológico.

5) Control Interno

a. Velar por que los riesgos de seguridad de la información sean gestionados adecuadamente por las oficinas y despachos judiciales y elevar los resultados obtenidos, acciones o estrategias, cuando así corresponda al Consejo Superior.

Tel.: 2295-3386 Fax: 2257-0412 Correo: tecnologia-info@poder-judicial.go.cr

Política	PL-SGSI-001	**Fecha actualización:**	26/10/2019	**Página #:**	5 de 7
Título:	Política de Seguridad de la Información				

6) Subcomité Institucional de Seguridad de la Información

a. Mediar en los conflictos en materia de seguridad de la información y los riesgos asociados, para así proponer soluciones.

b. Coordinar con los comités de Continuidad y de Riesgos de la institución, para mantener alineada toda la estrategia institucional.

c. Mantener informada a la Comisión Gerencial de Tecnologías de Información y Comunicaciones y Administración Superior sobre cualquier oportunidad de mejora, así como de los incidentes importantes y su respectiva solución en el Sistema de Gestión de la Seguridad de la Información.

d. Establecer los procedimientos tanto de priorización, así como de solución a los diferentes incidentes y riesgos que se vinculen con los activos de la información de la institución.

e. Promover la gestión de la seguridad a lo interno de todo el Poder Judicial.

7) Persona Usuaria

a. Cumplir con las pautas establecidas en las políticas y/o lineamientos de seguridad de la información.

8) Jefaturas de oficina

a. Velar por el cumplimiento de las políticas, lineamientos y demás elementos relativos a la seguridad de la información institucional, en sus respectivas oficinas.

b. Comunicar oportunamente a la DTIC los incumplimientos a la políticas, lineamientos y demás elementos sobre la seguridad de la información institucional.

6.0 PAUTAS

Para asegurar que se gestione correctamente la seguridad de la información en toda la institución, el Poder Judicial debe:

a. Definir y mantener un Sistema de Gestión de Seguridad de la Información (SGSI) que permita identificar las necesidades de la institución y las expectativas de las partes interesadas en materia de seguridad, incluyendo los requisitos legales, regulatorios y contractuales aplicables.

b. Desarrollar y aplicar todas las políticas, lineamientos y/o reglamentos de seguridad de la información necesarios, que permitan la protección adecuada de la información institucional y que apoyen el cumplimiento de esta política.

Tel.: 2295-3386 Fax: 2257-0412 Correo: tecnologia-info@poder-judicial.go.cr

c. Documentar y mantener actualizadas las responsabilidades y autoridades asociadas al SGSI, tanto de las personas que laboran para la organización, como de terceras relacionadas.

d. Definir un enfoque sistemático para la gestión de riesgos de seguridad de la información, donde los riesgos sean identificados, evaluados y tratados hasta que puedan ser aceptados por la institución, de acuerdo con el nivel de tolerancia al riesgo acordado.

e. Concientizar y capacitar a todas las personas que trabajan para la institución en materia de seguridad, confidencialidad y riesgos asociados con el uso de las TI, incluyendo las políticas y/o lineamientos y sus responsabilidades relacionadas con la seguridad de la información.

f. Implementar los procesos requeridos para la gestión de la seguridad de la información, y los relacionados con la operación de los controles de seguridad para tratar los riesgos identificados.

g. Monitorear el entorno de riesgo y tomar las acciones necesarias, para que los riesgos de seguridad de la información originados por cambios en el contexto de la institución puedan ser aceptados.

h. Evaluar el desempeño de la seguridad de la información y la efectividad del SGSI, para asegurar que sea conveniente, suficiente y cumpla con las necesidades y requisitos de la institución.

i. Tomar las acciones necesarias para asegurar la mejora continua del SGSI.

7.0 MEDICIÓN DEL CUMPLIMIENTO

El cumplimiento de esta política se verificará mediante diferentes métodos, entre los que se destacan: recorridos periódicos, auditorías internas y externas, reportes de las jefaturas, o cualquier otro mecanismo definido por la Dirección de Tecnología de Información y Comunicaciones.

8.0 EXCEPCIONES

Cualquier excepción a esta política debe ser aprobada previamente por Corte Plena o quien ésta designe como responsable para la aprobación de la misma.

Tel.: 2295-3386 Fax: 2257-0412 Correo: tecnologia-info@poder-judicial.go.cr

9.0 INCUMPLIMIENTOS

Cualquier persona que labore, visite o brinde apoyo al Poder Judicial y que no cumpla con lo aquí estipulado, queda sujeta a las sanciones disciplinarias y/o legales que los órganos correspondientes determinen. La Dirección de Tecnología de Información y Comunicaciones elaborará un informe donde se incluya un análisis de los riesgos derivados del incumplimiento, así como del posible impacto asociado.

10.0 DOCUMENTACIÓN RELACIONADA

- Normas técnicas para la gestión y control de las Tecnologías de Información de la Contraloría General de la República.
- Reglamento del Gobierno, de la Gestión y el uso de los Servicios Tecnológicos del Poder Judicial.
- Políticas y/o lineamientos de carácter específico o de segundo nivel que forman parte del Sistema de Gestión de Seguridad de la Información.

11.0 HISTORIAL DE VERSIONES

Fecha	Revisión #	Descripción del cambio	Responsable
22/06/2018	1.0	Política elevada a aprobación de Corte Plena	Comisión Gerencial de TI
26/10/2019	1.1	Acuerdo XXIII tomado por la Corte Plena, en la sesión N° 42-19 celebrada el 7 de octubre. Comunicado mediante circular de Secretaría de la Corte 197 – 2019.	Corte Plena-Aplicado por DTIC