SE REPRODUCE POR ERROR

**CIRCULAR N° 344-2023**

**Asunto:** Reglamento del Gobierno, de la Gestión y del uso de los servicios tecnológicos del Poder Judicial.

**A LOS SERVIDORES, SERVIDORAS, DESPACHOS JUDICIALES DEL PAÍS,**

**ABOGADOS, ABOGADAS Y PÚBLICO EN GENERAL**

**SE LES HACE SABER QUE:**

La Corte Plena en sesión N° 56-2023, celebrada el 27 de noviembre de 2023, artículo XXVI dispuso aprobar el Reglamento del Gobierno, de la Gestión y del uso de los servicios tecnológicos del Poder Judicial, el cual queda de la siguiente manera:

“Reglamento del Gobierno, de la Gestión y del uso de los servicios tecnológicos del Poder Judicial.

Capítulo I

Disposiciones generales

1. Objeto: El presente reglamento tiene por objeto establecer las normas que regirán el gobierno, gestión y uso de las tecnologías de información y comunicaciones en el Poder Judicial de la República de Costa Rica, con el fin de garantizar la protección de la información, la continuidad de los servicios institucionales, así como el mejor aprovechamiento y utilización de las tecnologías de información y comunicaciones en pro del cumplimiento de los objetivos institucionales.
2. Ámbito de aplicación: Este reglamento se aplicará a todas las personas usuarias internas del Poder Judicial (colaboradores) que accedan o interactúen con los medios tecnológicos que el  Poder Judicial pone a su disposición para la realización de sus labores (servicios, sistemas, plataforma tecnológica, y cualquier otro), así como a cualquier tercero sean personas usuarias de la administración de justicia  físicas o jurídicas usuarias externas, contratistas o cualquiera que tenga acceso a los sistemas informáticos, páginas web u otras tecnologías de información y comunicaciones dispuestas por la institución.
3. De los aspectos no previstos en el reglamento. Los aspectos no previstos en este reglamento se regularán por lo que dispone la Ley Orgánica del Poder Judicial, la Ley General de Control Interno, las Políticas de Tecnologías de Información y Comunicaciones del Poder Judicial, y demás ordenamiento jurídico en lo que sea aplicable.
4. Principios rectores: Los principios rectores que rigen el gobierno, la gestión y el uso de las tecnologías de información en el Poder Judicial son los siguientes:
5. Seguridad de la información: Todas las personas usuarias externas, el personal colaborador del Poder Judicial, los contratistas y cualquier tercero que haga uso de los servicios tecnológicos y canales digitales deben tomar medidas razonables para proteger la información, los sistemas e infraestructuras tecnológicas contra posibles amenazas, como el acceso no autorizado, el robo de información y la pérdida de datos.
6. Privacidad: El Poder Judicial se compromete a proteger la privacidad de las personas usuarias y a cumplir con todas las leyes y regulaciones aplicables en materia de privacidad y protección de datos al hacer uso de las TIC.
7. Transparencia: El Poder Judicial se compromete a proporcionar a las personas usuarias tanto internas como externas, información clara y completa sobre el uso de sus datos y a ser transparente en sus prácticas de recolección y procesamiento de datos.
8. Confidencialidad: La información sensible que conste en los sistemas institucionales tendrá carácter confidencial y solo podrá ser empleada para fines públicos y conforme al motivo que originó su suministro por la persona titular de la información.
9. Responsabilidad: Todas las personas usuarias y personal del Poder Judicial (colaboradores), así como cualquier tercero sean personas físicas o jurídicas usuarias externas, contratistas o cualquiera que tenga acceso y haga uso de los servicios tecnológicos sean estos sistemas informáticos, páginas web u otras tecnologías de información y comunicaciones, son responsables de cumplir con las políticas y los procedimientos de TI establecidos en este reglamento y otros lineamientos institucionales y responderán por el uso que se dé a la información, los servicios tecnológicos y las herramientas de trabajo que el Poder Judicial disponga.
10. Definiciones: Para los efectos de este reglamento, se deben tener en cuenta las siguientes definiciones y abreviaturas:
11. Amenaza: Es cualquier persona, gesto o acción que se anticipa a la intención de causar algún tipo de daño.
12. Canales Electrónicos: son las plataformas digitales y aplicaciones móviles que el Poder Judicial pone a disposición de la persona usuaria externa para que ésta pueda realizar transacciones, realizar consultas u obtener información de sus trámites en el tiempo y forma que así lo deseen sin necesidad de desplazarse a una oficina o despacho judicial.
13. Conducta inapropiada: Ejecución de acciones que vayan en contra de las buenas costumbres, así como también de las mejores prácticas. Todo aquello que atente contra la dignidad, la ética o los principios morales, así como en contra de las disposiciones y reglamentación del Poder Judicial.
14. Contraseña (Clave): Conjunto de caracteres alfanuméricos o sea letras mayúsculas, minúsculas, números y caracteres especiales, escogidos de forma secreta por la persona usuaria u operadora de los servicios informáticos, utilizada para acceder a los diferentes aplicativos o sistemas informáticos. Dicha contraseña es personal y no deber ser de manejo público.
15. Correo Masivo: Mensaje que se envía a un grupo considerablemente grande de contactos a la misma vez.
16. Dispositivo electrónico: Se denomina así a todo aquel aparato en el cual se combinen componentes electrónicos, con el fin de aprovechar las señales eléctricas. Estos dispositivos utilizan la electricidad para almacenar y transformar la información. Se pueden dar algunos ejemplos tales como: computadores portátiles, agendas electrónicas, teléfonos celulares, “tablets”, dispositivos de almacenamiento externo.
17. Gestión en Línea, página web del Poder Judicial transaccional y la aplicación móvil: son los canales electrónicos transaccionales o de consulta al que las personas usuarias externas pueden acceder en los horarios que el Poder Judicial establezca y desde cualquier sitio para para obtener la información y realizar las transacciones en los trámites y servicios que el Poder Judicial brinde.
18. Identidad de la persona Usuaria: La identidad de la persona usuaria o bien como lo citan en diversas fuentes ID, es un código alfabético que identifica de forma única a una persona inscrita en la red del Poder Judicial y se utiliza para acceder a los diferentes sistemas informáticos, dicha identificación es personal e intransferible, de igual forma la identidad de la persona usuaria se utiliza para auditar el acceso a dichos sistemas y otros recursos tecnológicos.
19. Incidente de Continuidad: Interrupción no planificada de un sistema/servicio de tecnología de información o un proceso crítico de negocio que afecta la operación normal, superando el tiempo establecido para la recuperación (RTO) establecido.
20. Información crítica para el funcionamiento del despacho: Se dice que la información es crítica para una oficina cuando la misma es necesaria para llevar a cabo determinada función u ofrecer algún servicio, además de ser requerida para evaluar el cumplimiento de las diferentes tareas asignadas al personal.
21. Información sensible para el funcionamiento del despacho: Información privada de un individuo o la institución, cuya divulgación podría tener un efecto negativo en su propietario, por ejemplo, datos personales, resoluciones que involucren a una persona menor de edad, entre otros.
22. Información pública: Cualquier tipo de dato que sea generado o resguardado por quien ejerza una función o potestad pública y que no tenga su acceso restringido por ley.
23. Infraestructura Tecnológica: Elementos necesarios para operar y gestionar el entorno de TI en la institución, por ejemplo; el hardware, el software, los elementos de red, un sistema operativo (SO) y el almacenamiento de datos.
24. Software malicioso (Malware): La palabra es una abreviatura de su nombre en inglés “Malicious Software” la cual comprende todo tipo de virus, programas espías, gusanos, entre otros, los cuales son una secuencia de código malicioso que se inserta en un archivo, sin consentimiento de la persona que opera la computadora, para afectar el correcto funcionamiento de los recursos tecnológicos.
25. Personas usuarias o usuarios (Colaboradoras): son las personas que laboran para el Poder Judicial y utilizan las herramientas tecnológicas, los sistemas y las infraestructuras para la realización de sus labores cotidianas como parte de la gestión interna institucional.
26. Personas usuarias externa o usuarios externos: es la persona física o jurídica que se encuentre vinculada con el Poder Judicial y la cual podrá utilizar todos los contenidos que la institución disponga en los CANALES ELECTRONICOS.
27. Plan de Recuperación de Desastres (DRP): Colección documentada de procedimientos e información que guían a la DTIC y las áreas tecnológicas del OIJ a responder, recuperar, reanudar y restaurar a un nivel de operación aceptable predefinido luego de un incidente de continuidad.
28. Programas (software): Se puede definir como programa al conjunto de aplicaciones diseñadas e instaladas en las computadoras utilizadas para realizar funciones específicas de forma que sean útiles para las personas que las operan. Es el componente intangible, pero necesario para que el equipo funcione.
29. Recursos tecnológicos: Son los componentes o dispositivos tanto de hardware (recursos tangibles como computadoras, tabletas, discos portables, 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.
30. Red Interna (Intranet): Red Informática privada restringida para el uso de un grupo de personas específico; por ejemplo, las personas usuarias de una organización, de un edificio o de un conjunto de oficinas.
31. Red Internacional (Internet): Es un conjunto descentralizado de redes de comunicación que permite la comunicación entre diferentes computadores y de sistemas informáticos independientes.
32. Reglamento: Documento con reglas sobre algún tema. Para el caso de esta normativa, se entenderá como el presente " Reglamento del Gobierno, de la Gestión y del uso de los servicios tecnológicos del Poder Judicial".
33. Riesgo: Es la probabilidad de que una amenaza se materialice y cause un daño o perjuicio.
34. Sistemas de comunicación electrónica: Se puede definir como la transmisión, recepción y aprovechamiento de la información de un lugar a otro, para lograrlo se utilizan dispositivos y programas previamente configurados para estos fines. La información puede ser escrita, de voz o de video. Por ejemplo: correo electrónico, videoconferencias, chat, entre otros.
35. Uso personal: Acciones realizadas por las personas usuarias utilizando los recursos tecnológicos de la institución, en actividades no relacionadas con las funciones asignadas dentro del Poder Judicial.
36. Acrónimos:
37. CGTI: Comisión Gerencial de Tecnologías de la Información.
38. CSJ: Corte Suprema de Justicia.
39. 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 para lograr la protección de la Información.
40. DTIC: Dirección de Tecnologías de Información y Comunicaciones.

Capítulo II

Instancias de gobierno y gestión de las tecnologías de información y comunicaciones en el Poder Judicial

Sección I

De los órganos de Gobierno de tecnologías de información y comunicaciones

1. Responsables del gobierno institucional de TI. La Corte Plena, el Consejo Superior y la Comisión Gerencial de Tecnologías de Información y Comunicaciones, son los responsables de velar por el adecuado gobierno de las tecnologías de información y comunicaciones en el Poder Judicial.
2. Responsabilidades de la Corte Plena en el modelo de Gobierno. Corresponde a la Corte Plena, como máximo órgano de decisión y gobierno institucional:
3. Valorar y aprobar el marco orientador en materia de gobierno y gestión tecnológica que permita la definición de las prioridades de las estrategias, proyectos e inversiones institucionales con el fin de cumplir con los objetivos propuestos y generar el valor público.
4. Definir los principios que permitan establecer la priorización institucional en materia tecnológica, de forma tal que la Dirección de Tecnologías de Información y Comunicaciones logre desarrollar y poner en marcha las acciones, planes y presupuestos que respondan a esas necesidades, objetivos y oportunidades institucionales.
5. Analizar y aprobar las propuestas de planificación estratégica tecnológica que realice la Dirección de Tecnologías de Información y Comunicaciones, así como las modificaciones que surjan durante su ejecución.
6. Aprobar el presupuesto en materia tecnológica.
7. Dar el debido respaldo en términos de recursos materiales, humanos y presupuestarios a las iniciativas y proyectos tecnológicos una vez que hayan sido incorporados como parte de la planificación tecnológica institucional.
8. Analizar los riesgos estratégicos que en materia tecnológica pueda estar enfrentando el Poder Judicial y contribuir con la Dirección de Tecnologías de Información y Comunicaciones en establecer las medidas y estrategias de gestión que permitan minimizar los impactos asociados.
9. Aprobar las políticas y el reglamento que regula y norma el gobierno y gestión tecnológica que le proponga la Dirección de Tecnologías de Información y Comunicaciones.
10. Aprobar las modificaciones al presente reglamento que le proponga la Dirección de Tecnología de Información o Comunicaciones o la Comisión Gerencial de Tecnologías de Información y Comunicaciones.
11. Responsabilidades del Consejo Superior. Corresponde al Consejo Superior del Poder Judicial como máximo órgano administrativo del Poder Judicial:
12. Asignar los recursos humanos que se requieran para el desarrollo de proyectos institucionales que incorporen la tecnología.
13. Aprobar los lineamientos administrativos que permitan una adecuada gestión tecnológica institucional.
14. Conceder audiencia a la Dirección de Tecnologías de Información y Comunicaciones con el fin de analizar las propuestas, alcances y limitaciones de la gestión tecnológica institucional.
15. Contribuir con la Corte Plena en el análisis de los riesgos estratégicos tecnológicos.
16. Contribuir con la Corte Plena en la definición de principios que permitan una adecuada priorización de las necesidades tecnológicas y por ende de la construcción de soluciones que los soporten.
17. Informar oportunamente a la Dirección de Tecnologías de Información y Comunicaciones sobre cualquier cambio en las prioridades institucionales y evaluar las propuestas que para el cumplimiento le realice la DTIC.
18. Analizar los riesgos operativos que en materia tecnológica pueda estar enfrentando el Poder Judicial y contribuir con la Dirección de Tecnologías de Información y Comunicaciones en establecer las medidas y estrategias de gestión que permitan minimizar los impactos asociados.
19. Cualquier otra función que en materia de gobierno institucional de tecnologías le asigne le Corte Plena.
20. Responsabilidades de la Comisión Gerencial de Tecnologías de Información y Comunicaciones. Corresponde a la Comisión Gerencial de TI, aquellas responsabilidades y funciones que le confiere el presente reglamento en la Sección II, así como cualquier otra que en su momento defina la Corte Plena.

Sección II

De la Comisión Gerencial de Tecnologías de la Información

1. La Comisión Gerencial de Tecnologías de Información y Comunicaciones. La Comisión Gerencial de Tecnologías de la Información (CGTIC) es una comisión de carácter especial en cumplimiento de lo definido en las Normas Técnicas para el gobierno y gestión de las TIC definidas por el Ministerio de Ciencia y Tecnología como ente rector nacional en la materia y será el órgano encargado de avalar y elevar las propuestas en temas de Estrategia Tecnológica y desarrollo tecnológico del Poder Judicial a la Corte Plena, una vez que sea definida y propuesta por la Dirección de Tecnologías de Información y Comunicaciones.

La Comisión Gerencial de Tecnologías de la Información es un órgano asesor y recomendativo de la Corte Plena y del Consejo Superior según corresponda y de conformidad con las competencias de cada órgano.

1. Funciones de la CGTIC. La CGTI tendrá como funciones y atribuciones:
2. ~~A~~valar y elevar las propuestas que sobre el desarrollo institucional de tecnologías de información y comunicaciones realice la Dirección de Tecnologías de Información y Comunicaciones, 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; así como establecer criterios orientadores para el avance tecnológico, tomando en cuenta para ello aspectos de oportunidad, prioridad, calidad y costo-beneficio.
3. Revisar y avalar las políticas tecnológicas que defina la Dirección de Tecnologías de Información y Comunicaciones y elevarlas a la Corte Plena para que constituyan el marco de referencia del accionar de la función tecnológica.
4. Revisar y avalar los lineamientos administrativos que defina la Dirección de Tecnologías de Información y Comunicaciones y elevarlos al Consejo Superior para su aprobación y divulgación.
5. Dar seguimiento y apoyo a la gestión tecnológica, así como al presupuesto global institucional en esta materia.
6. Revisar y elevar a la Corte Plena las políticas que promuevan la innovación, la modernización y el uso inteligente de las tecnologías de la información en la gestión judicial, en procura de un servicio de calidad hacia la persona usuaria, de conformidad con lo que la Dirección de Tecnologías de Información y Comunicaciones defina como ente rector en la materia.
7. Avalar el Plan estratégico de las Tecnologías de Información y Comunicaciones que la Dirección de Tecnologías de Información y Comunicaciones desarrolle, así como las estrategias, proyectos y planes estratégicos, táctico y operativos en materia tecnológica, y revisar su correcto alineamiento con el plan estratégico institucional.
8. Velar por una efectiva y oportuna comunicación de la Dirección de Tecnologías de Información y Comunicaciones y la organización en general.
9. Mantener informada en conjunto con la Dirección de Tecnología de Información y Comunicaciones a la Corte Plena y al Consejo Superior sobre el avance y los resultados de los proyectos aprobados en el Plan Estratégico de TI.
10. Revisar y avalar el anteproyecto de presupuesto anual que en materia tecnológica le presente la Dirección de Tecnología de Información y Comunicaciones.
11. Cualquier otra función que le sea asignada por la Administración Superior.
12. Integración de la CGTIC. La Comisión Gerencial de Tecnologías de la Información estará integrada por las siguientes personas:
13. La Presidencia de la Corte Suprema de Justicia o quien ésta designe, quien ejercerá el rol de coordinar la Comisión.  Sin embargo, quien ejerza la presidencia de la Comisión, podrá delegar en otra persona de su elección, este rol.
14. Por una Magistrada o Magistrado representante de cada una de las Salas de la Corte Suprema de Justicia.
15. Por una persona integrante del Consejo Superior.
16. Por el Director o Directora del Despacho de la Presidencia.
17. Por el Director o Directora de la Dirección de Tecnologías de Información y Comunicaciones.
18. Por el Director o Directora Ejecutiva.
19. Por la Directora o Director de la Dirección de Planificación.
20. Por la Directora o Director de Gestión Humana.
21. Por la Directora o Director del Organismo de Investigación Judicial.
22. Por la Fiscala o Fiscal General
23. Por la Jefatura de la Defensa Pública.
24. Por la Jefatura del Centro de Apoyo a la Gestión.
25. Por la Secretaria o Secretario de la Corte Suprema de Justicia.

Las áreas integrantes de la Comisión deberán nombrar una persona que las sustituya en su ausencia, a fin de evitar suspensiones de las sesiones de dicho órgano.

Este nombramiento deberá ser comunicado a la Dirección de Tecnologías de Información y Comunicaciones en su calidad de Secretaría de la Comisión Gerencial.

De igual manera, podrá contarse con la participación de asesores externos a la organización, cuando la Comisión lo considere necesario. Los invitados tendrán derecho a voz, pero no a voto.

La Dirección de Tecnologías de Información y Comunicaciones, llevará el control de las agendas, las actas y de la ejecución de los acuerdos.

1. Coordinación de la CGTIC. La Comisión Gerencial de Tecnologías de la Información será coordinada por la Presidencia de la Corte Suprema de Justicia, o bien a quien ésta designe.
2. De las sesiones de la CGTIC. La Comisión Gerencial de Tecnologías de la Información podrá sesionar en forma ordinaria y extraordinaria.  Las sesiones ordinarias se realizarán bimensualmente, en la hora y lugar que así lo disponga la persona que coordine de la Comisión.

Las sesiones extraordinarias se realizarán por convocatoria de la Coordinación de la Comisión Gerencial de Tecnologías de la Información, por medio de la Dirección de Tecnologías de Información y Comunicaciones, cuando la índole de los asuntos sea urgente, y se tramitarán los puntos para los que fue convocada, y aquellos que en el seno se estime conveniente por mayoría absoluta de los miembros.

También, podrá sesionar a criterio de la Presidencia de la Comisión o de su Secretaría, utilizando medios electrónicos como el correo electrónico, sistemas de videoconferencia o cualquier otra tecnología que para tales efectos se disponga.

1. Del quórum para sesionar. La Comisión Gerencial de Tecnologías de la Información podrá sesionar válidamente con la presencia de al menos cinco de sus miembros, sean estos titulares o suplentes y los acuerdos serán adoptados por mayoría simple de los presentes. En caso de empate, se someterá nuevamente a votación en la sesión siguiente.
2. De las funciones de la coordinación. La CGTI estará a cargo de una presidenta o un presidente, quien dirigirá las sesiones; y para esos efectos tiene las siguientes funciones:
3. Convocar a las sesiones ordinarias y extraordinarias, de forma directa o a través de la Secretaría de la Comisión.
4. Presidir las sesiones de la Comisión.
5. Abrir y cerrar las sesiones. También las podrá suspender, cuando lo considere procedente, por motivos de conveniencia y oportunidad.
6. Dirigir los debates y poner a votación los asuntos.
7. En coordinación con la Secretaría de la Comisión, comunicar los acuerdos a la Administración Superior, así́ como a las dependencias que corresponda.
8. En coordinación con la Secretaría de la Comisión, llevar el control de la ejecución de los acuerdos.
9. Representar, en conjunto con la Secretaría de la Comisión Gerencial, a la CGTI en todas aquellas actividades donde se deba contar con la participación de este órgano, así́ como actuar como intermediario entre la Corte Plena y la CGTI, para todos aquellos asuntos que le competan.
10. De las funciones del Director o Directora de la DTIC en la CGTIC.  A la Dirección de Tecnologías de Información y Comunicaciones, a través de su Director o Directora, le corresponderá asumir un rol preponderante en las sesiones de la Comisión y ejercerá un liderazgo técnico en el análisis, discusión de los asuntos que sean del conocimiento de la Comisión. Entre otras cosas, le corresponderá:
11. Proponer la planificación estratégica tecnológica, los cambios a ésta y los avances sobre su ejecución.
12. Proponer los portafolios, programas y proyectos que estime pertinentes tanto estratégicos como operativos e informar sobre el avance de su ejecución.
13. Informar sobre la gestión tecnológica institucional.
14. Alertar sobre los riesgos estratégicos y operativos vinculados con la gestión tecnológica institucional.
15. Definir y presentar los presupuestos que en materia tecnológica se requieran para la adecuada sostenibilidad y desarrollo de proyectos tecnológicos.
16. Proponer estrategias de atención y mitigación de amenazas a las que se enfrente la infraestructura tecnológica institucional.
17. Cualquier otra función dentro de su ámbito de competencia.

Será obligatoria su participación en las sesiones y en caso de que no asista, participará el subdirector o subdirectora de DTIC.  Le corresponde además elaborar el orden del día de los asuntos que deba conocer la CGTI.

1. De las responsabilidades de los integrantes de la CGTI. Las personas que integran la CGTI deberán asumir sus tareas con responsabilidad, analizar los temas de la agenda de previo a las sesiones, investigar y prepararse para las discusiones y hacer propuestas sobre temas y proyectos relacionados con tecnología.  Además, su participación a las sesiones es obligatoria, salvo que motivo justificado lo impida, situación ante la cual deberán nombrar una persona suplente.  Sus actuaciones se regirán por este reglamento y demás ordenamiento y lineamientos que sean aplicables.
2. De la designación de equipos de trabajo. La CGTI como órgano colegiado, designará los equipos de trabajo que sean necesarios para realizar las actividades de análisis y estudio, brindar la asesoría y los apoyos necesarios para coadyuvar la toma de decisiones. Estos equipos de trabajo serán coordinados por la persona que así designe la CGTI.

Sección III

Del órgano responsable de la gestión tecnológica

1. Órgano rector en materia de tecnologías de información y comunicaciones: La Dirección de Tecnologías de Información y Comunicaciones es el órgano rector en materia tecnológica del Poder Judicial.
2. Deber de acatar lo que la DTIC disponga. Las áreas tecnológicas del OIJ, sean la Plataforma de Información Policial y la Unidad Tecnológica Informática, así como cualquier otra área institucional que se defina por el Consejo Superior o la Corte Plena para que gestione tecnologías de información y comunicaciones para sus respectivos ámbitos, deben adherirse a los principios, políticas, marcos, guías, procedimientos e infraestructuras tecnológicas; incluyendo aspectos como modelos y arquitecturas aprobadas; metodologías para la gestión de proyectos tecnológicos; estandarización de la infraestructura tecnológica (programación, bases de datos, reutilización de código fuente, entre otros elementos); esto con el fin de propiciar un adecuado ambiente de control y facilitar los procesos de verificación y cumplimiento.

Todas las oficinas que gestionen tecnología en el Poder Judicial responderán técnicamente a la Dirección de Tecnologías de Información y Comunicaciones.

1. Responsabilidad de regular el desarrollo y la gestión tecnológica institucional. La Dirección de Tecnologías de Información y Comunicaciones, es la responsable de formular y proponer a la Corte Plena, o el órgano que ésta designe, los elementos normativos que regulen el gobierno y la gestión tecnológica del Poder Judicial.

Como órgano rector en materia de tecnologías de información y comunicaciones, la DTIC queda facultada para definir principios, políticas, lineamientos y demás modelos que faciliten la gestión tecnológica institucional y propiciar su aprobación por los órganos correspondientes, esto incluye la definición de marcos de trabajo para la construcción de planes estratégicos tecnológicos, metodologías para la gestión de proyectos tecnológicos, modelos y arquitecturas para la construcción de soluciones, la seguridad informática y otros instrumentos que permitan el desarrollo y mejor aprovechamiento de las TIC en el Poder Judicial.

1. Del alineamiento de la gestión con el gobierno de TI. Con el objeto de gestionar, coordinar, fomentar y obtener el máximo aprovechamiento por el uso de las tecnologías de información y comunicaciones en el Poder Judicial, la Dirección de Tecnologías de Información y Comunicaciones se alineará a lo establecido por los órganos de gobierno de TI.

Para ello, deberá formular las propuestas que técnicamente resulten viables para la valoración del Consejo Superior en lo administrativo y de la Corte Plena en lo estratégico, debiendo alinear la estrategia tecnológica con la estrategia institucional en procura del cumplimiento de los objetivos, metas y políticas institucionales, para lo cual debe elaborar, dar seguimiento y mantener actualizado un plan estratégico de tecnologías.

1. Superior jerárquico de la DTIC. La Dirección de Tecnologías de Información y Comunicaciones dependerá del Consejo Superior y es un órgano asesor de la Corte Plena en lo que al gobierno, gestión y desarrollo tecnológico se refiere.

Cuando la Corte Suprema de Justicia se avoque el conocimiento de una competencia del Consejo Superior en el campo de las tecnologías de la información, dicha Dirección estará sometida a la autoridad y lineamientos de la Corte Plena.

1. De los proyectos tecnológicos. Todo proyecto que implique el desarrollo y construcción de soluciones tecnológicas, sean éstas de infraestructura o de soluciones de software, deberá ser aprobado por la Dirección de Tecnologías de Información y Comunicaciones y contar con su visto bueno, así como también deberá contar con dictamen favorable de la Comisión Gerencial de Tecnologías de la Información, de previo a la respectiva aprobación por parte del órgano decisor.

La Dirección de Tecnologías de Información y Comunicaciones es la encargada de ejecutar las actividades relacionadas a la construcción de soluciones tecnológicas de aquellos proyectos que hayan sido aprobados por la Corte Plena o el Consejo Superior, para lo cual se le debe:

1. Definir los marcos metodológicos específicos para la priorización de proyectos tecnológicos.
2. Establecer las metodologías y marcos de trabajo para la gestión y desarrollo de proyectos en materia tecnológica.
3. Gestionar el portafolio de proyectos y los programas relacionados, que permitan dar cumplimiento a la estrategia institucional y tecnológica.
4. Dar informes periódicos sobre la gestión de proyectos tecnológicos a la Comisión Gerencial de Tecnologías de Información y Comunicaciones.
5. Colaborar en aquellos proyectos que, aunque no siendo administrados directamente por la DTIC, utilicen la tecnología de información como elemento estratégico para el cumplimiento de los objetivos del área ejecutante y conforme a una planificación institucional previa. El componente tecnológico desarrollado como parte de proyectos institucionales, se gestionará según los modelos definidos por la Dirección de Tecnologías de Información y Comunicaciones.

Si alguna oficina desea desarrollar un proyecto que involucre tecnologías de la información, debe:

1. Plantearlo como parte de los ejercicios de formulación presupuestaria, siguiendo los lineamientos establecidos.
2. Si el proyecto involucra una donación, antes de la misma, debe remitir la solicitud, el estudio de factibilidad, información técnica y demás documentos correspondientes, para el análisis y aval de la DTIC y la Comisión Gerencial de Tecnologías de la Información, con el fin de asesoras en lo correspondiente al Consejo Superior para su debida aprobación.
3. En caso de necesidades urgentes que no formen parte de este proceso de formulación, deben remitir la solicitud, el estudio de factibilidad y demás documentos correspondientes, para el análisis y aval de la DTIC y la Comisión Gerencial de Tecnologías de la Información, con el fin de posteriormente ser llevados ante el Consejo Superior para su debida aprobación.
4. Atención de necesidades institucionales. La Dirección de Tecnologías de Información y Comunicaciones está en la obligación de generar productos y servicios de TI, de conformidad con las necesidades de las diferentes oficinas que conforman el Poder Judicial, de acuerdo con las posibilidades presupuestarias, prioridades establecidas, recurso humano y tecnológico disponible, manteniendo en todo momento un enfoque de mejora continua.
5. De la gestión de riesgos tecnológicos. La Dirección de Tecnologías de Información y Comunicaciones deberá desarrollar y mantener un plan de gestión de riesgos mediante el cual la institución pueda responder adecuadamente a las diferentes amenazas que puedan afectar el correcto funcionamiento de las TI.

La Dirección de TI debe comunicar periódicamente los riesgos tecnológicos existente a la CGTIC, el Consejo Superior y a la Corte Plena, según sea el caso, con el fin de que, en el ejercicio de sus competencias, estos órganos ejecuten las acciones que correspondan.

En caso de que las medidas de mitigación dependan de otras oficinas dentro del Poder Judicial, éstas deberán prestar la colaboración con el fin de que los servicios tecnológicos y los institucionales no se vean impactados negativamente ante la materialización de los riesgos.

1. Alineamiento entre seguridad de la información y seguridad informática. La Dirección de Tecnologías de Información y Comunicaciones, se alineará a las políticas y directrices establecidas por el Consejo Superior y por la Corte Plena en lo referente a la seguridad de la información y será responsable por la seguridad informática institucional.

Para ello, la DTIC definirá los lineamientos administrativos, los marcos de trabajo y demás elementos que permitan una protección razonable de la información en medios tecnológicos.

Todas las personas que interactúen con los servicios tecnológicos, independientemente de si laboran para la institución o si son personas usuarias externas, deberán cumplir con los lineamientos sobre seguridad informática que se definan.

1. Responsabilidad de velar por el conocimiento sobre la seguridad informática. La Dirección de Tecnologías de Información y Comunicaciones y el Consejo Superior, deberán velar porque todo el personal de la organización conozca las regulaciones de seguridad informática, a fin de evitar el error humano y el uso inapropiado de los recursos tecnológicos. Para esto deberá realizar lo siguiente:

Es competencia de las jefaturas o coordinaciones de cada oficina, velar por el cumplimiento de las directrices institucionales en materia de seguridad informática.

1. De la seguridad informática en la construcción de soluciones tecnológicas. La Dirección de Tecnologías de Información y Comunicaciones deberá velar por la integridad de la información digital en todos los procesos de implementación de las nuevas aplicaciones, así como en los procesos de mantenimiento de software e infraestructura; para lograr esto la Dirección de Tecnologías de Información y Comunicaciones deberá:
2. Definir previamente los requerimientos de seguridad que deben ser considerados en la implementación y mantenimiento de software e infraestructura.
3. Contar con procedimientos claramente definidos para el mantenimiento y puesta en producción del software e infraestructura.
4. Mantener un acceso restringido y los controles necesarios sobre los ambientes de desarrollo, mantenimiento y producción.
5. Controlar el acceso al código fuente y a los datos de prueba.
6. Velar porque las aplicaciones de software que desarrolla permitan en la medida de las posibilidades institucionales almacenar información íntegra, de forma confidencial y que esté disponible en el momento en que se requiera.
7. Resguardar y no divulgar las medidas de seguridad cibernética establecidas para la protección de las bases de datos. Estas medidas deberán ser revisadas y actualizadas al menos una vez al año o cuando se presente algún evento que requiera la actualización de estas.
8. Aplicar las medidas de seguridad informática necesarias ante el surgimiento de nuevas amenazas.
9. De la continuidad de los servicios tecnológicos. La Dirección de Tecnologías de Información y Comunicaciones deberá desarrollar y mantener planes y documentación que permitan realizar un manejo razonable de la continuidad de los servicios tecnológicos que brinda al Poder Judicial. Como mínimo debe generar:

a. Plan de gestión de crisis y comunicaciones de TI.

b. Plan de recuperación de desastres (DRP).

c. Un plan de evaluación de riesgos tecnológicos.

d. Documentación sobre la criticidad de los recursos de TI.

La DTIC, debe formular y proponer ante el Consejo Superior y la Corte Plena, las estrategias vinculadas con tecnologías de información y comunicaciones que permitan cumplir con los objetivos de continuidad institucionales definidos en el modelo institucional de gestión de la continuidad.

1. Del Plan Estratégico de Tecnologías de Información y Comunicaciones) PETIC. La Dirección de Tecnologías de Información y Comunicaciones, es el órgano responsable de implementar y mantener las Tecnologías de Información necesarias y en relación con el marco estratégico institucional establecido, debe:
2. Desarrollar un plan estratégico de tecnologías de información y comunicaciones (PETIC) alineado al Plan Estratégico Institucional, el cual será revisado y aprobado por Corte Plena.
3. Alinear constantemente el PETIC a la visión institucional y a las necesidades de los diversos grupos de interés, documentando los cambios y propiciando el mejor aprovechamiento de los recursos tecnológicos institucionales.
4. Solicitar a la Corte Plena los recursos presupuestarios, que se requieran para el cumplimiento de los proyectos estratégicos tecnológicos que se definan y de acuerdo con la priorización de estos.
5. Solicitar al Consejo Superior, los recursos humanos y materiales que sean necesarios para la correcta ejecución de los proyectos institucionales en materia tecnológica.
6. Definir y comunicar los riesgos tecnológicos estratégicos vinculados con la ejecución de las actividades, proyectos y operaciones relacionadas con el PETIC.

Deberán contribuir con la creación, ejecución y seguimiento del PETIC, todas aquellas oficinas que gestionan tecnologías y se encuentran debidamente facultadas para hacerlo, como la Plataforma de Información Policial y la Unidad de Tecnologías de Información del OIJ.

1. Otras oficinas que gestionan tecnología. La Plataforma de Información Policial y la Unidad de Tecnologías de Información, así como las dependencias que se definan institucionalmente para la gestión tecnológica, serán los responsables de adquirir, administrar, dar soporte técnico y mantener actualizada la infraestructura tecnológica y los sistemas que desarrollen, además de velar por el buen funcionamiento de esta en el Poder Judicial.

Además, estarán sometidos a los lineamientos técnicos que defina la Dirección de Tecnologías de Información y Comunicaciones.

1. Del software permitido para uso institucional. La Dirección de Tecnologías de Información y Comunicaciones, así como el personal que éste designe, son los únicos autorizados para instalar, actualizar y desinstalar software o programas en los equipos del Poder Judicial.

Únicamente se podrán instalar herramientas que sean parte de la lista de software base autorizado por la DTIC. Cualquier necesidad específica que se tenga y que no esté incluida en esta lista, deberá ser aprobada por la Dirección de Tecnologías de Información y Comunicaciones de previo a su instalación.

Para estas tareas, deberá respetarse lo siguiente:

1. La Dirección de Tecnologías de Información y Comunicaciones tiene la responsabilidad de publicar en la intranet la lista de software permitido en el Poder Judicial para realizar las funciones diarias.
2. La lista de software permitido en el PJ estará constituida únicamente por software licenciado que cumple con la normativa de derechos de autor vigente en el país, o bien software gratuito previamente analizado y autorizado por esta Dirección.
3. Desarrollo de sistemas y soluciones tecnológicas. La Dirección de Tecnologías de Información y Comunicaciones o las áreas definidas institucionalmente como la PIP y la UTI, son las responsables del desarrollo de sistemas de información, soluciones tecnológicas y otras infraestructuras a utilizar en el Poder Judicial. Para lo cual debe:
4. Establecer los controles y asignar las funciones, responsabilidades y permisos de acceso al personal a cargo de las labores de implementación y mantenimiento de software.
5. Controlar la implementación del software en el ambiente de producción y garantizar el traslado de los datos fuente utilizados en los programas para los procesos de conversión y migración.
6. Definir los criterios para determinar la procedencia de cambios y accesos de emergencia al software y datos, y los procedimientos de autorización, registro, supervisión y evaluación técnica, operativa y administrativa de los resultados de esos cambios y accesos.
7. Controlar las distintas versiones de los programas que se generen como parte de su mantenimiento.
8. Analizar alternativas de solución de acuerdo con criterios técnicos, económicos, operativos y jurídicos, y lineamientos previamente establecidos.
9. Contar con una definición clara, completa y oportuna de los requerimientos, como parte de los cuales se debe incorporar aspectos de control, seguridad y auditoría bajo un contexto de costo – beneficio.
10. Definir metodologías para la priorización en la atención de las necesidades de mejoras en los sistemas.
11. No obtener ni suministrar información a terceros contenida en las infraestructuras que custodian.
12. Incidentes en los servicios tecnológicos. Es responsabilidad de la Dirección de Tecnologías de Información y Comunicaciones la detección, análisis y resolución de forma oportuna de los problemas e incidentes que se presenten en lo referente a su plataforma tecnológica.

De igual forma, la Plataforma de Información Policial, la PIP y cualquier otro órgano que esté aprobado para gestionar las TIC en el Poder Judicial, deberán dentro de su ámbito de competencia, atender los incidentes que se presenten.

Con la información obtenida se levantará una base de datos de conocimiento que minimice el riesgo de recurrencia y almacene toda la información obtenida.

1. Contrataciones en materia tecnológica. La Dirección de Tecnologías de Información y Comunicaciones debe velar por obtener de forma satisfactoria los objetivos contratados a terceros en lo que corresponde a actualizaciones, implementaciones, asesorías y mantenimiento de la infraestructura tecnológica o aplicaciones.

No están autorizadas las contrataciones en materia tecnológica que no cuenten con el visto bueno de la Dirección de Tecnologías de Información y Comunicaciones.

Cuando la contratación se gestione por un área diferente a la DTIC, aunque se cuente con el visto bueno correspondiente, corresponderá al área que ejecuta la contratación, garantizar que se cumplan los objetivos institucionales, así como los lineamientos, prácticas, modelos de trabajo y demás elementos que permitan integrar las soluciones a la arquitectura de sistemas, de infraestructura y de datos del Poder Judicial.

1. Recursos de revocatoria. En caso de existir disconformidad ante lo resuelto técnicamente por la Dirección de Tecnologías de Información y Comunicaciones, cabrá recurso de revocatoria ante la misma Dirección y de apelación ante el Consejo Superior.

Capítulo IV

De los servicios tecnológicos y herramientas informática para la gestión institucional.

Sección Primera

Usos de los recursos tecnológicos institucionales.

1. Del uso permitido de los servicios tecnológicos. Los servicios y recursos tecnológicos deberán utilizarse únicamente para propósitos laborales. No está permitido el uso de éstos para fines personales o comerciales. En el ejercicio de sus facultades, las personas usuarias (Colaboradoras) deben velar por:
2. Actuar de manera consistente con los valores compartidos en lo que al uso de los recursos tecnológicos y los servicios puestos a su disposición se refiere.
3. No interferir con la productividad o el desempeño laboral de las personas servidoras judiciales, así como demás personas usuarias.
4. No afectar de forma negativa el desempeño de los recursos tecnológicos.
5. No violar las disposiciones o políticas institucionales, leyes nacionales o internacionales.
6. No afectar la imagen del Poder Judicial.
7. Uso responsable de las tecnologías y servicios tecnológicos. Las jefaturas de las oficinas como las personas subordinadas a éstas deberán utilizar racionalmente y para los fines laborales para los que fueron otorgados, los servicios de correo electrónico e Internet, así como el uso de los sistemas de información y equipos computacionales y cualquier otro servicio tecnológico.

En caso de que la jefatura detecte algún incumplimiento por parte de las personas subordinadas, debe tomar las medidas administrativas correspondientes, de conformidad con lo dispuesto en este reglamento, en las políticas aprobadas por la Administración Superior y los lineamientos técnicos que emita la Dirección de Tecnologías de Información y Comunicaciones.

1. Asignación de derechos de acceso a internet y correo electrónico. La asignación de acceso a los servicios de Internet y correo electrónico, se realizará previa autorización de la jefatura de mayor rango de sus respectivos ámbitos, o bien de las personas que estas deleguen para estos fines.  El nombre de las personas comisionadas para ejecutar esta labor debe ser comunicado oficialmente a la Dirección de Tecnologías de Información y Comunicaciones.

La aplicación de la autorización estará a cargo de la Dirección de Tecnologías de Información y Comunicaciones o las áreas tecnológicas que ésta designe, la cual valorará la factibilidad técnica con base en las capacidades institucionales y siempre salvaguardando la seguridad informática de la institución, creará el acceso correspondiente a los servicios autorizados, generando a partir de ese momento la responsabilidad sobre su debido uso.

1. Movimientos del personal y permisos de acceso a los servicios tecnológicos. Las jefaturas inmediatas deberán notificar oportunamente al área de tecnología correspondiente, cualquier movimiento que se realice en las personas usuarias a su cargo (ascenso, destitución, jubilación, suspensión, defunción) con el fin de deshabilitar temporal o permanentemente los permisos para acceso los servicios tecnológicos de la institución.

Por su parte, las jefaturas inmediatas son responsables de mantener al día los permisos y credenciales de las personas usuarias en los sistemas de información, utilizando para ello las herramientas que la Dirección de Tecnologías de Información y Comunicaciones facilite.

El uso indebido de estas credenciales será responsabilidad de la jefatura respectiva y de aquella persona que no desactivó o actualizó la condición de la persona usuaria (Colaboradora).

1. Asignación y registro de activos tecnológicos. La asignación, registro y movimiento de activos tecnológicos se regirá por el Reglamento para el registro, control y uso de activos institucionales del Poder Judicial.
2. Inventario de equipos tecnológicos. Las jefaturas y/o personas autorizadas formalmente por éstas, son los responsables de mantener un inventario actualizado de los equipos tecnológicos asignados a las oficinas bajo su cargo.  Esto con el fin de poder llevar un control cruzado con los inventarios generados por la Dirección de Tecnologías de Información y Comunicaciones y así tener un control más exacto de los recursos tecnológicos asignados a las distintas oficinas a nivel nacional.

La obligación de realizar inventarios aquí establecida es sin detrimento del control de activos que debe realizarse siguiendo los lineamientos del Departamento de Proveeduría.

1. Ingreso y salida de activos tecnológicos. Las jefaturas y/o personas autorizadas por éstas, deberán controlar y registrar el ingreso y salida de los activos tecnológicos asignados a la oficina a su cargo, así como reportar y coordinar ante las instancias respectivas cualquier falla que se pueda presentar en dichos equipos, en los sistemas de información y en otros servicios tecnológicos. A las personas que por sus funciones se les asigne equipo portátil propiedad de la institución deberán atender lo estipulado en el artículo 60 de este Reglamento.
2. Respaldos de información. Las jefaturas deberán velar por que toda información digital que a criterio de la propia de la oficina se considere sensible y crítica para el funcionamiento del despacho se almacene en los servidores, mecanismos y sistemas de información que el Poder Judicial disponga oficialmente.

El respaldo de la información almacenada en los servidores y sistemas de información será responsabilidad de la Dirección de Tecnologías de Información y Comunicaciones y de las áreas tecnológicas autorizadas.

La información almacenada en las computadoras de escritorio, las portátiles, los dispositivos de almacenamiento portables o equipos de respaldo personal, no será respaldada ni custodiada por la Dirección de Tecnologías de Información y Comunicaciones y áreas tecnológicas adscritas a esta. En caso de pérdida, la responsabilidad recaerá sobre la persona que tiene asignado el equipo.

La información que las oficinas coloquen en servicios de almacenamiento en la nube, no serán respaldadas por la Dirección de Tecnologías de Información y Comunicaciones.

De tener información sensible y crítica para la oficina que se deba respaldar, es responsabilidad de cada oficina colocarla en los servidores y aplicaciones que la Dirección de Tecnologías de Información y Comunicaciones destine para tales fines.

1. Monitoreo de los servicios tecnológicos. El Poder Judicial tendrá la potestad de monitorear mediante los mecanismos que la Dirección de Tecnologías de Información y Comunicaciones disponga, el uso de los recursos y servicios tecnológicos.

Las actividades de monitoreo se podrán realizar de forma cotidiana para garantizar el adecuado funcionamiento de los servicios o de forma más intensiva cuando exista sospecha de que se esté frente a un comportamiento atípico para la seguridad informática o la continuidad de los servicios tecnológicos y de las operaciones institucionales.  No obstante, no podrá acceder a la información del contenido de los correos o de otra información de carácter personal almacenada en las computadoras, sin el consentimiento previo de la persona usuaria o por orden de un juez o jueza de la República.

Sección Segunda

Del correo electrónico.

1. Buzón de correo electrónico. El buzón de correo electrónico que el Poder Judicial ponga a disposición de las personas usuarias deberá utilizarse únicamente para los fines laborales para los cuales está dispuesto.
2. Responsabilidad de las cuentas de correo electrónico. Las personas usuarias son las responsables de cualquier actividad que se pueda realizar desde las cuentas asociadas a sus buzones de correo, por lo que no deben permitir que otras personas utilicen estas cuentas de correo electrónico.

En caso de que se detecten usos indebidos, las personas usuarias tienen la obligación de reportarlos inmediatamente a su superior para que se inicie con las medidas correspondientes.

La persona a la que la cuenta de correo electrónico esté asignada, es responsable de mantener las buenas prácticas en lo que al uso del correo se refiere (no abrir correos de dudosa procedencia, publicidad, entre otros), esto con el fin de evitar en la medida de lo posible que los mensajes que reciba o envíe no contengan virus, para lo cual sus programas de antivirus deben estar activos y actualizados, esto sin detrimento de que el Poder Judicial implemente mecanismos de protección.

Es responsabilidad de cada persona usuaria, comunicar al área tecnológica correspondiente, a través de los mecanismos de reportes de incidentes y solicitudes destinados para tal fin, cuando por algún motivo se presente un inconveniente que le permita cumplir con lo aquí estipulado.

1. Tamaño del buzón de correo electrónico. Con el propósito de evitar saturaciones que puedan afectar el buen funcionamiento del servicio, el tamaño máximo de los mensajes que se pueden enviar está limitado, fijándose dicho límite en función de los recursos disponibles en cada momento.

La Dirección de Tecnologías de Información y Comunicaciones será la responsable de definir con base en criterios técnicos el tamaño máximo de los mensajes de correo y de comunicarlo institucionalmente.

1. Prohibiciones en el uso del correo electrónico. No está permitido:
2. Utilizar las cuentas de correo del Poder Judicial para el envío de publicidad.
3. Usar el servicio de correo electrónico de forma que interfiera con el rendimiento del servicio o con las labores propias del Poder Judicial.

Sección Tercera

De la Internet suministrada por la institución.

1. Servicio de Internet. Las personas autorizadas para acceder a los servicios de Internet e Intranet deberán cumplir con lo siguiente:
2. Respetar la privacidad de otras personas usuarias.  No está permitido obtener copias intencionales de archivos, códigos, contraseñas o información ajena; ni suplantar a otra persona en una conexión que no le pertenece o enviar información a nombre de otra persona sin consentimiento expreso del titular de la cuenta.
3. No utilizar los servicios de Internet suministrada por la institución para fines personales, como, por ejemplo: juegos en línea, radio o televisión por Internet, publicación de contenidos personales, sitios de ocio, sitios para adultos, sitios de descarga de contenidos maliciosos, así como otros sitios que la Dirección de Tecnologías de Información y Comunicaciones o las instancias superiores dispongan para salvaguardar la seguridad y el desempeño del personal.
4. Salvo los casos donde por la naturaleza de la oficina así se requiera, no acceder a sitios con contenido sexual o pornográfico, ni bajar o ver material inapropiado, no solo referido a juegos, música y pornografía, sino a cualquier otro material inaceptable, que atente contra los principios morales, sociales y en general que no se relacionen con los objetivos de la institución. En resumen, debe utilizarse única y exclusivamente para propósitos laborales.
5. Filtrado de sitios web. La Dirección de Tecnologías de Información y Comunicaciones será la responsable de implementar mecanismos automatizados y de ciberseguridad que permitan proteger la información digital de la institución de los riesgos externos que se encuentran en Internet, por lo que queda facultada a filtrar la navegación a los sitios de Internet en función del contenido de las páginas o sitios que se visitan, a través de herramientas especializadas para ello, las siguientes son las premisas básicas de este filtrado:

a. Sitios permitidos: Se permitirá la navegación en aquellos sitios que estén referidos a búsqueda de información necesaria para la elaboración, ampliación o referencia de temas relacionados con el trabajo, siempre y cuando no comprometan la seguridad informática institucional.

b. Sitios bloqueados: Se bloquearán aquellos sitios que se cataloguen de acuerdo con su contenido y que contengan pornografía, redes sociales, chats, juegos de entretenimiento, azar y apuestas, sitios racistas y de odio, música y video, transferencia de cualquier tipo de archivos a través de mensajería, servicios de radio y TV por demanda y todos aquellos que no estén asociados a los propósitos laborales del Poder Judicial.  De igual manera, se bloquearán todos aquellos sitios que no aparezcan catalogados o cuya agrupación sea desconocida.

c. Desbloqueo de sitios: Si por razones laborales plenamente justificadas se requiere el desbloqueo temporal o permanente de algún sitio, debe presentarse ante la Dirección de Tecnologías de Información y Comunicaciones la solicitud avalada por la jefatura de mayor rango de sus respectivos ámbitos, o bien las personas que éstas deleguen para estos fines.

La Dirección de Tecnologías de Información y Comunicaciones analizará la solicitud en términos del impacto a la seguridad informática y a la continuidad de la infraestructura institucional y habilitará el acceso cuando corresponda.  Aun así, la persona solicitante y la máxima autoridad que avala la solicitud, asumirán la responsabilidad de cualquier evento o incidente que se presente.

Sección Cuarta

Del equipo de cómputo institucional.

1. Asignación de equipos. Los equipos computacionales (de escritorio, portátiles o laptops, tabletas, teléfonos inteligentes) propiedad de la institución, serán asignados con el objetivo de cumplir sus funciones y de conformidad con lo establecido en el Reglamento de Activos Fijos.
2. Uso adecuado de los equipos de cómputo. La persona usuaria tiene la responsabilidad de utilizar adecuadamente el equipo de cómputo y los periféricos que se le asignen, así́ como de la información almacenada en este. De igual manera, la jefatura de la oficina tiene la responsabilidad de velar por el uso adecuado de todos los equipos computacionales asignados a la oficina.
3. Responsabilidad de la jefatura o encargado de oficina. La jefatura de oficina tiene la responsabilidad de asegurar que el equipo computacional permanezca dentro de sus instalaciones, salvo que su salida sea plenamente justificada, sea para mantenimiento del equipo, por traslados entre oficinas o por sustitución del equipo computacional, debiendo dejar registro de cada uno de estos movimientos.

Se excluye de esta responsabilidad el equipo computacional portátil, por asignarse este directamente a las personas, salvo en los casos en que este tipo de equipos se asigne directamente a la oficina. En este caso, todo lo relativo a los equipos portátiles, será tratado conforme lo establezca el Reglamento para el registro, control y uso de activos del Poder Judicial.

La jefatura de oficina debe comunicar estos movimientos a la Administración correspondiente, quien a su vez lo hará de conocimiento de La Dirección de Tecnologías de Información y Comunicaciones.

1. Limpieza externa de los equipos asignados. La persona usuaria a la que se le haya asignado equipo computacional en cualquiera de sus modalidades: computadora de escritorio, computadora portátil, tableta, discos duros externos, entre otros, es responsable de su limpieza externa, la cual debe ser realizada periódicamente, así como del cuido, para lo cual debe verificar que los productos a utilizar sean para la limpieza de equipo de oficina y computación.
2. Comunicación de fallas o desperfectos en los equipos. Las personas usuarias a las que se les asigne equipo computacional están en la obligación de informar a la Dirección de Tecnologías de Información y Comunicaciones o áreas tecnológicas correspondientes sobre cualquier falla o desperfecto tanto físico (hardware) como lógico (software), que presente el equipo con el fin de proceder con su revisión y de ser necesario su reparación.  Este reporte, debe generarse siguiendo los procedimientos que estas dependencias definan.

En caso de desperfectos o daños causados a los equipos computacionales asignados, ya sea por falta de cuido o intencionalmente, la persona responsable asumirá los costos por la reparación o sustitución de los equipos, siguiendo para ello el debido proceso.

1. Del traslado de equipos portátiles. La persona usuaria que tenga asignados equipos móviles de la institución (computadoras portátiles, tabletas, discos duros externos, o cualquier otro dispositivo propiedad del Poder Judicial), queda autorizada para trasladar el equipo a su discreción y será responsable directo del equipo, respondiendo por cualquier daño o desperfecto que esta sufra o por la pérdida de información contenida en los dispositivos. En caso de vacaciones, incapacidades y otros movimientos del personal, deberá contemplarse lo que señale el Reglamento para el registro, control y uso de activos del Poder Judicial y otros lineamientos para la reasignación temporal del equipo.
2. Seguro para los equipos portátiles. Es responsabilidad del Poder Judicial, asegurar ante las instancias pertinentes, las computadoras portátiles y otros dispositivos móviles de su propiedad.
3. Sustracción o pérdida de equipo. En caso de sustracción o pérdida del equipo, la persona que tenga asignado el mismo debe interponer la denuncia correspondiente, sin detrimento de las acciones administrativas asociadas.  De igual manera, tiene el deber de informarlo a la Jefatura de oficina.
4. Prohibición de modificar los componentes de los equipos. Queda totalmente prohibido a la persona usuaria, realizar modificaciones o alteraciones al equipo tecnológico, porque esta práctica anularía los términos de la garantía y la persona asumirá las responsabilidades económicas y administrativas correspondientes.

La Dirección de Tecnologías de Información y Comunicaciones y las áreas tecnológicas que ésta designe, serán los responsables de darle mantenimiento a los componentes internos del equipo.

Sección Quinta

De las redes de comunicaciones.

1. Responsabilidad de gestión de las redes de datos. La Dirección de Tecnologías de Información y Comunicaciones es responsable de la instalación y gestión de las redes internas de datos.  Queda completamente prohibido a las oficinas o personas usuarias instalar, desinstalar o manipular redes de datos sin la debida autorización por escrito de la Dirección de Tecnologías de Información y Comunicaciones.

Ninguna persona usuaria deberá permitir el acceso a la red interna de la institución a personas externas a la misma o a personal no autorizado, mediante el uso de la cuenta que le ha sido asignada.

1. Analizadores de red. El uso de analizadores de red es permitido única y exclusivamente por el personal de la Dirección de Tecnologías de Información y Comunicaciones, con el fin de monitorear la funcionalidad de la red institucional.  Todas las demás personas usuarias, tienen prohibida la realización de este tipo de actividades.
2. Software de espionaje y malicioso. No está permitido la instalación o uso de software de espionaje, monitoreo de tráfico o programas maliciosos en la red de datos que originen: violaciones a la seguridad, interrupciones de la comunicación en red, que eviten o intercepten la autenticación de la persona usuaria (inicio de sesión en el dominio) por cualquier método, o que busquen acceder a recursos a los que no se les ha permitido expresamente el acceso.
3. Suspensión de la cuenta. Cuando se detecte un uso no aceptable en las redes del Poder Judicial o en los servicios internos o externos que presta, se cancelará la cuenta o se desconectará temporal o permanentemente a la persona usuaria o la red involucrada dependiendo de la severidad del incidente. La reconexión se hará́ en cuanto se considere que el uso no aceptable se ha suspendido.

La Dirección de Tecnologías de Información y Comunicaciones, remitirá a las autoridades correspondientes, los informes que permitan iniciar las sanciones administrativas dependiendo de la severidad del incidente ocasionado.

Sección Sexta

De los sistemas de información y el software

1. Propiedad de los sistemas de información. Todos los programas de software desarrollados o adquiridos por el Poder Judicial, sea por gestión interna, compra, donación o cesión son propiedad de la institución y mantendrán los derechos que la ley de propiedad intelectual le confiera.
2. Respeto de los derechos de autor. Las personas usuarias tienen prohibida la copia o distribución, para fines personales o comerciales, de cualquier aplicación o software protegido legalmente o violar cualquier derecho de autor o términos de licenciamiento adquiridos por la institución.
3. Revisión del software instalado. La Dirección de Tecnologías de Información y Comunicaciones, es responsable de realizar revisiones periódicas para asegurar que sólo software con licencia y autorizado esté instalado en las computadoras de la institución.  Producto de esta revisión, podrá iniciar los procedimientos administrativos correspondientes.
4. Actualización de información en los sistemas. Las personas usuarias de los sistemas de información tienen la responsabilidad de mantener actualizada la información y asegurar la completitud de esta.
5. Autorización para el desarrollo de sistemas. Las personas usuarias no están autorizadas a desarrollar o adquirir por su parte este tipo de herramientas, sin contar con la autorización expresa de la Dirección de Tecnologías de Información y Comunicaciones.
6. Uso de metodologías aprobadas por la Dirección de Tecnología para el desarrollo y construcción de soluciones tecnológicas. El desarrollo y construcción de soluciones tecnológicas se realizará en apego a la estrategia institucional definida y aprobada, utilizando las metodologías de priorización y de gestión de proyectos que la Dirección de Tecnologías de Información y Comunicaciones defina, así como los esquemas y arquitecturas que resulten más convenientes para los objetivos institucionales, de forma tal que se maximice el uso de los recursos humanos, presupuestarios y materiales.

Capítulo V

De la Seguridad Informática

Sección Primera

Deberes de la Dirección de Tecnologías de Información y Comunicaciones.

1. Instalaciones físicas donde se instalan las infraestructuras tecnológicas. La Dirección de Tecnologías de Información y Comunicaciones, en conjunto con las instancias correspondientes, debe vigilar que las condiciones físicas y ambientales donde se encuentran instalados los diferentes recursos tecnológicos utilizados para brindar servicios, sean seguras. Para lo cual se deben tomar en consideración los siguientes puntos:
2. Definir las necesidades físicas y ambientales donde se instalarán los equipos e infraestructura tecnológica.
3. Mantener la documentación actualizada sobre la ubicación física de los diferentes equipos utilizados para brindar servicios (servidores, switch, routers y otros equipos utilizados en la infraestructura tecnológica de la institución).
4. Establecer un control de acceso para terceros ajenos a la institución, con el fin de evitar en lo posible el error humano o bien el mal manejo de los equipos.

Corresponde a la Dirección Ejecutiva a través del Departamento de Servicios Generales y las Administraciones Regionales, dotar de las condiciones necesarias para un funcionamiento adecuado de las instalaciones físicas donde se instalen servicios e infraestructuras tecnológicas.

1. Herramientas para el análisis y detección de usos indebidos. La Dirección de Tecnologías de Información y Comunicaciones pondrá en funcionamiento herramientas de control automatizadas para analizar y detectar los usos y comportamientos indebidos o ilícitos en la red, sin que se violenten los derechos constitucionales de libertad de expresión y privacidad de las comunicaciones.
2. Respeto a la privacidad de las personas usuarias. Es responsabilidad de la Dirección de Tecnologías de Información y Comunicaciones respetar en todo momento la privacidad de las personas usuarias y no divulgar información acerca de las cuentas de acceso del uso que haga del servicio a menos que sea requerido para cumplir con procedimientos legales por orden de una autoridad competente.

La DTIC es responsable de la custodia de la información institucional almacenada en los medios tecnológicos que administra y tiene expresamente prohibido suministrarla, sin el debido consentimiento del despacho que gestiona la información o de una orden judicial.

1. Suspensión de servicios en caso de fallas a la seguridad informática. En caso de que la Dirección de Tecnologías de Información y Comunicaciones identifique una falla de seguridad en un recurso tecnológico, podrá suspender el acceso a los servicios de comunicaciones electrónicas e Internet, mientras ésta es corregida, para evitar problemas adicionales que se puedan ocasionar mientras se elimina la falla detectada.

Sección Segunda

Deberes de las jefaturas y/o encargados de las oficinas.

1. De los movimientos de personal y las credenciales de acceso. Las jefaturas, coordinadores o el personal autorizado oficialmente, deberán notificar, en la medida de lo posible, con al menos una semana de antelación a la Dirección de Tecnologías de Información y Comunicaciones, cualquier movimiento que se realice en el personal a su cargo, sea por contratación, ascenso, destitución, solicitud de nuevas cuentas de acceso, extensiones de permisos, entre otros, con el fin de gestionar dichos permisos para el acceso a los recursos de la red.
2. De las cuentas de correo e internet. Las jefaturas deberán solicitar a la Dirección de Tecnologías de Información y Comunicaciones, con previa autorización por parte de la jefatura de mayor rango de sus respectivos ámbitos, o bien la persona que esta delegue para estos fines, la creación y activación de cuentas de correo electrónico e Internet y credenciales de acceso a los recursos tecnológicos institucionales. La activación de este tipo de servicios está directamente relacionada con el perfil del puesto que las personas desempeñan y a la factibilidad técnica para lograrlo. En caso de que el servicio no esté asociado al puesto, deberá ser solicitado por la jefatura de mayor rango.

La jefatura inmediata de la persona tiene la responsabilidad de crear las credenciales de ingreso a los sistemas de información que se utilizan en su oficina y velará por el uso de esas credenciales, la información y los recursos tecnológicos institucionales.

1. Responsabilidad sobre las cuentas de usuario. Las jefaturas, coordinaciones o el personal autorizado oficialmente, deberán tener un control cruzado con la Dirección de Tecnologías de Información y Comunicaciones en lo que a las cuentas de servicio se refiere, ya que las mismas no deben ser utilizadas para iniciar sesiones de trabajo a menos que exista una justificación previa, para tales fines, a cada funcionario se le asigna una cuenta de acceso personal y una palabra clave o contraseña (password).

Sección Tercera

Deberes de las personas usuarias (Colaboradores).

1. Responsabilidades principales de las personas usuarias. Las personas usuarias deberán seguir las directrices institucionales que eviten la introducción de software malicioso (malware) o la manipulación indebida de la información a través de medios informáticos. Por tanto, cuando se utilice el acceso a Internet, los sistemas de información, las comunicaciones electrónicas, las memorias removibles y otros servicios tecnológicos, deberán:
2. Utilizar la Internet y los sistemas de comunicación electrónica de acuerdo con las disposiciones que emita este reglamento y que se definan en los lineamientos institucionales a través de la Dirección de Tecnologías de Información y Comunicaciones, el Consejo Superior o la Corte Plena.
3. Mantener las condiciones de seguridad de los sistemas, incluyendo la confidencialidad de las palabras claves y cualquier otro sistema o plataforma institucional o fuera de ésta que en virtud de sus labores tenga acceso.
4. Ejecutar la revisión de software malicioso (malware) a los dispositivos (discos portables USB) externos antes de acceder a su información, haciendo uso de las herramientas tecnológicas proveídas por el Poder Judicial.
5. Resguardar la información de carácter confidencial, de acceso restringido, o aquella que goce de protección por los derechos de autor o sea de uso exclusivo del Poder Judicial, a la que tenga acceso; quedando estrictamente prohibido comunicarla o facilitarla, directa o indirectamente a un tercero sin la debida autorización de alguna autoridad competente.
6. Abstenerse de utilizar o descargar documentos o archivos que no tengan relación alguna con sus labores habituales.
7. Cualquier otra que sea definida y comunicada por la Dirección de Tecnologías de Información y Comunicaciones para garantizar un uso adecuado de los servicios tecnológicos.
8. Uso de información por parte de las personas usuarias. Las personas servidoras del Poder Judicial deberán hacer un buen uso, desecho y reutilización de medios electrónicos o impresos que contengan información institucional, de acuerdo con el grado de confidencialidad de la información.
9. Uso de las cuentas de acceso por parte de las personas usuarias. Las cuentas de acceso asignadas y el uso que se haga de las mismas, se regirá por las siguientes disposiciones:
10. Cada persona usuaria se le proporcionará un identificador y contraseña personal para acceder a los recursos tecnológicos del Poder Judicial. Esta identificación digital se le asignará de acuerdo con el perfil de su puesto.
11. La contraseña es estrictamente de uso personal y por tanto confidencial. En ningún caso es permitido compartirla o cederla a terceros, aun cuando los propósitos sean laborales.
12. Cada persona usuaria será responsable de las acciones que se reporten ejecutadas con su identificador digital y contraseña, asumiendo las consecuencias de las actuaciones que resulten de su uso.
13. Si la persona usuaria sospecha que alguien más está haciendo uso de su clave debe reportarlo de inmediato y cambiar la clave.
14. En caso de cualquier olvido la única persona autorizada para proporcionar una nueva clave y/o contraseña es el administrador de la red designado por la Dirección de Tecnologías de Información y Comunicaciones u otras áreas tecnológicas.
15. Se deberá cambiar la contraseña de acuerdo con las políticas establecidas por la Dirección de Tecnologías de Información y Comunicaciones.
16. No podrá realizar acciones orientadas a infiltrarse, dañar o atacar la seguridad de la información del Poder Judicial ni de otra institución pública y organización privada, a través de medio físico o electrónico alguno.
17. No podrá dar a conocer códigos de seguridad tales como contraseñas a terceros, o entorpecer por ningún medio el funcionamiento de los servicios y telecomunicaciones del Poder Judicial.
18. No utilizar programas que vulneren la seguridad de los equipos y servidores del Poder Judicial.
19. No dañar o alterar las características técnicas de los servicios tecnológicos provistos por la Dirección de Tecnologías de la Información y Comunicaciones y otras áreas tecnológicas.
20. Respetar la protección legal otorgada a programas, textos, artículos y bases de datos, según la legislación internacional sobre propiedad intelectual y las normas pertinentes de nuestro país.
21. En toda comunicación electrónica, la persona usuaria deberá mantener los cuidados, profesionalismo y discreción que guarda con los documentos o memorandos impresos.
22. Responsabilidad sobre la información en unidades de red. Las personas usuarias son responsables de la información almacenada en las unidades de red y no deberán utilizarlas para guardar archivos de música (mp3, WAV, wma, etc.), fotos o videos de uso personal (avi, mpg, wmv, mov, etc.).

Capítulo VI

De las Prohibiciones y régimen disciplinario.

1. Prohibiciones. Queda prohibido utilizar los recursos tecnológicos del Poder Judicial a todo el personal en general para realizar actividades de índole personal y que no formen parte de sus funciones diarias.

Adicionalmente queda prohibido:

1. El acceso del personal no técnico a lugares restringidos como centros de datos, salas de servidores, centros de comunicación o cuartos de comunicación en todos los circuitos y oficinas judiciales del país, a menos de que se trate de labores de mantenimiento previamente agendadas y autorizadas por la DTIC, o bien en caso de emergencia siempre y cuando se encuentre en compañía de personal de la Dirección de Tecnologías de Información y Comunicaciones.
2. Contratar de forma privada o instalar redes de Internet en las oficinas sea para el uso personal o laboral sin la aprobación de la Dirección de Tecnologías de Información y Comunicaciones. Tampoco se permite la manipulación de la infraestructura de redes existente, la instalación de enrutadores o repetidores de red o cualquier otro dispositivo que no esté autorizado.
3. Almacenar productos o artefactos (latas de pintura, papeles, productos de limpieza, equipo para arreglar, escaleras, cajas, tubos fluorescentes, equipo de oficina, mobiliario, entre otros), en los centros de datos, salas de servidores, centros de comunicación o cuartos eléctricos en todos los circuitos, excepto los respectivos extintores.
4. Conectar electrodomésticos (microondas, radios, coffee makers, refrigeradores, etc.)  a los tomacorrientes utilizados para los equipos de cómputo.
5. Conectar dispositivos personales (Tablet, computadores personales, celulares, reproductores de música, etc.) a la red institucional.
6. Ejecutar proyectos relacionados con tecnologías de la información sin que hayan pasado por el proceso de evaluación por parte de la Dirección de Tecnologías de Información y Comunicaciones y la Comisión Gerencial de Tecnologías de la Información.
7. La copia o distribución (física y electrónica) de información institucional de carácter confidencial o de acceso restringido, así como aquella que esté protegida por derechos de autor o sea de uso exclusivo del Poder Judicial.
8. El acceso, copia, impresión, almacenamiento o divulgación de información con contenido pornográfico, racista, sexual o cualquier material que atente contra la dignidad, la ética o los principios morales y que no sean propios de investigaciones o actuaciones judiciales.
9. Descargar, ejecutar o copiar programas de software no autorizados y contrarios a las políticas institucionales.
10. Asumir la identidad de otra persona, nombres falsos o anónimos.
11. Enviar correos que comprometan la imagen del Poder Judicial.
12. Enviar correos tipo "cadena" a uno o más destinatarios.
13. El envío de correos masivos. Se exceptúan de esta prohibición las oficinas expresamente autorizadas para este fin.
14. Instalar software no autorizado que se ejecute para funciones de espionaje, monitoreo de tráfico o programas en la red de datos que eviten o intercepten la autenticación de las cuentas de acceso (inicio de sesión en el dominio) por cualquier método o que busquen acceder a recursos a los que no se les ha permitido expresamente el acceso, originando esto violaciones a la seguridad e interrupciones de la comunicación en red de la institución.
15. Divulgar información sensible a personas no autorizadas con lo cual se comprometan las labores sustantivas que se llevan a cabo en materia tecnológica dentro del Poder Judicial.
16. Las demás prohibiciones que establezca y comunique oportunamente la Administración Superior para lograr un mejor uso de los recursos tecnológicos institucionales.
17. Aplicación del régimen disciplinario. Las infracciones al presente reglamento darán motivo para iniciar el correspondiente procedimiento administrativo disciplinario.

Capítulo VII

De los servicios institucionales para uso de las personas usuarias externas

1. De las personas usuarias externas. Entiéndase por persona usuaria externa, toda persona física o jurídica que interactúe con los servicios institucionales a través de una serie de canales electrónicos dispuestos por el Poder Judicial como parte de las facilidades para la consulta, tramitación, seguimiento y acceso a la información de una forma expedita y sin limitaciones geográficas o de horario.
2. De los canales electrónicos para uso de las personas usuarias externas. El Poder Judicial podrá poner a disposición de las personas usuarias físicas o jurídicas de la administración de justicia (personas usuarias externas) y otros servicios institucionales, una serie de servicios por canales que puede ser utilizados a través de la web, en dispositivos móviles como teléfonos inteligentes o tabletas, o a través de otras tecnologías que señale técnicamente la Dirección de Tecnologías de Información y Comunicaciones.

Estos servicios son un complemento de los servicios brindados por las oficinas y despachos judiciales y no los sustituyen.

1. Del horario de atención. Los servicios institucionales ofrecidos por la aplicación móvil operarán en forma gratuita y en horario de 24 horas, los 7 días de la semana, durante los 365 días del año según el horario de Costa Rica, salvo los casos donde se programen mejoras a la plataforma, a los sistemas o a los servicios que se brindan por los canales digitales, lo cual será comunicado de previo. También, el servicio podrá verse suspendido sin previo aviso sea por fallas internas o externas en las plataformas tecnológicas por las que se brindan los servicios.

Sin embargo, el Poder Judicial puede modificar este horario de disponibilidad, sin previo aviso, si lo considera conveniente, ya sea por razones de seguridad informática o por alguna otra razón interna.

1. Del acceso a los canales digitales. Para poder utilizar los servicios que el Poder Judicial brinda a través de sus canales electrónicos es necesario que las personas usuarias externas ingresen utilizando las credenciales y contraseñas que les emite la institución, las cuales son de uso personal e intransferible. De igual forma, podrán acceder utilizando la firma digital o cualquier otro medio que técnicamente se disponga.
2. De las credenciales y contraseña de acceso. Las credenciales y la contraseña de acceso constituyen la prueba irrefutable de que la persona usuaria externa es quien accedió a los servicios y aplicaciones brindados por los canales electrónicos del Poder Judicial y que todas las operaciones realizadas han sido aceptadas consciente y voluntariamente.

La persona usuaria externa a la que se le asignen estas credenciales se obliga a no compartir su contraseña con otra persona, ni a introducirla en robots o cualquier otra plataforma no conforme con lo que el Poder Judicial estipule, de hacerlo, asumirá la responsabilidad por el uso que se le dé, relevando al Poder Judicial de toda responsabilidad por tal hecho y asumiendo las responsabilidades correspondientes.

En caso de detectarse el uso contrario a lo dispuesto institucionalmente, el acceso a los servicios tecnológicos institucionales podrá suspenderse.

1. Del consentimiento informado al hacer uso de los canales digitales del Poder Judicial. Al solicitar las credenciales de acceso a los servicios digitales por canales electrónicos del Poder Judicial y con su uso, la persona usuaria externa entiende y brinda el consentimiento para la recolección de información y el análisis, tratamiento y uso de ésta en pro de la mejora de los servicios que se le otorgan por parte del Poder Judicial.

Como consecuencia, la persona usuaria externa de los Servicios digitales del Poder Judicial acepta lo dispuesto en la Ley de Protección de la Persona Frente al Tratamiento de sus Datos Personales Ley No. 8968 y su Reglamento, que da fe del conocimiento de la existencia de bases de datos en el Poder Judicial, donde se almacenarán datos personales, las cuales son de uso interno y no para comercializar la información.

1. Resguardo de información y credenciales de acceso. La persona usuaria, no debe suministrar a terceras personas, información asociada a los métodos de autenticación o esquemas de seguridad, tales como: contraseñas, PIN, códigos de seguridad, códigos de verificación, entre otros; y debe observar las más estrictas normas de confidencialidad y resguardo de su información personal y de seguridad.
2. Uso del servicio. Al hacer uso de los servicios por canales electrónicos, la persona usuaria externa solo debe acceder o tener acceso a los recursos informáticos, a través de medios autorizados y no debe utilizar mecanismos que pongan en riesgo la continuidad del servicio institucional (lo que incluye el uso de robots u otras herramientas automatizadas para consulta masiva y/o extracción de información de forma no autorizada y validada por el Poder Judicial).

De las Prohibiciones en el uso de los servicios institucionales para las personas usuarias externas.

1. Prohibiciones. Queda prohibido a las personas usuarias externas:
2. Utilizar los servicios tecnológicos del que el Poder Judicial facilite de forma contraria a como han sido diseñados.
3. El acceso, alteración o destrucción no autorizada, o cualquier intento de ello, a información del Poder Judicial o de otras personas usuarias.
4. La introducción de información, archivos y otros elementos que contengan software malicioso.
5. La introducción de las credenciales de acceso en sistemas de acceso masivo como robots u otras tecnologías que pongan en riesgo la continuidad de los servicios por canales electrónicos.
6. El préstamo de las contraseñas y credenciales de acceso.
7. El acceso a información sobre trámites que no sean los propios o que pertenezcan a un tercero sin el debido consentimiento.

El uso indebido de los canales electrónicos del Poder Judicial por parte de la persona usuaria externa, faculta al Poder Judicial a dar suspender temporal o de forma definitiva el acceso al servicio de esa cuenta.

Capítulo VII

Disposiciones Finales

1. Derogatorias. Se deroga el Reglamento del Gobierno, de la Gestión y del uso de los servicios tecnológicos del Poder Judicial, aprobado por la Corte Plena en la sesión celebrada el 19 de junio de 2017, artículo III. También se deroga el Reglamento Interno de la Comisión Gerencial de Tecnologías de la Información en el Poder Judicial costarricense, aprobado por la Corte Plena en la sesión N° 52-13, celebrada el 16 de diciembre del 2013, artículo XXIII.

El presente Reglamento rige a partir de su publicación en el *Boletín Judicial*.”

- 0 -

Publíquese una sola vez en el Boletín Judicial.

San José, 22 de diciembre de 2023.

**Licda. Silvia Navarro Romanini**

**Secretaria General**

**Corte Suprema de Justicia**

*Ref.:* 659-2017 / 8028-2023, 8048-2023, 9248-2023, 9348-2023

*CCV\**