Circular de Secretaría de la Corte N° 100 - 2017

22 de Junio del 2017

Fecha de Publicación: 12 de Julio del 2017

Descriptores/Temas: Tecnología

Es documento origen de: Circular de Secretaría de la Corte 070 del año 2019

Documentos citados: - **Circulares y Avisos**

Publicada en SECRETARÍA GENERAL DE LA CORTE N°100 del 22 de junio del 2017

CIRCULAR N° 100-2017

Asunto: **1.** Se deja sin efecto Circulares N° 120-2010 y 22-2014 del 6 de setiembre del 2010 y 3 de febrero de 2014, respectivamente. **2.** Modificación del "Reglamento de la Administración y el uso de los servicios Tecnológicos del Poder Judicial".-

A LAS AUTORIDADES JUDICIALES DEL PAÍS,
INSTITUCIONES, ABOGADOS Y PÚBLICO EN GENERAL

SE LES HACE SABER QUE:

La Corte Plena en sesión Nº 19-17 celebrada el 19 de junio de 2017, artículo III, dispuso hacer de conocimiento la aprobación de la modificación del "Reglamento de la Administración y el uso de los servicios Tecnológicos del Poder Judicial" que literalmente dice:

Reglamento del Gobierno, la Gestión y el uso de los servicios
Tecnológicos del Poder Judicial

Índice:

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

Capítulo I

Disposiciones generales

Artículo 1.- Este reglamento tiene por objeto regular la gestión de las tecnologías de información, mediante el establecimiento de normas estándar para la planificación, adquisición, implementación, soporte y uso de las tecnologías de información y comunicaciones en las diversas oficinas del Poder Judicial.

Artículo 2.- Las disposiciones contenidas en este reglamento son de cumplimiento obligatorio para todas las personas que laboran para el Poder Judicial, así como para quienes interactúen por cualquier medio tecnológico, con las oficinas del Poder Judicial.

Artículo 3.- Para los efectos de este reglamento, se deben tener en cuenta las siguientes definiciones y abreviaturas:

Administración Superior: Se refiere a la Corte Plena o el órgano que esta designe.

Amenaza: Una amenaza es cualquier persona, gesto o acción que se anticipa a la intención de causar algún tipo de daño.

CGTI: Comisión Gerencial de Tecnologías de la Información**.**

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.

Contraseña (Clave): Conjunto de caracteres alfanuméricos o sea letras mayúsculas, minúsculas y números, escogidos de forma secreta por el usuario u operador 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.

CSJ: Corte Suprema de Justicia.

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.

DTIC: Dirección de Tecnología de Información y Comunicaciones.

Identidad del Usuario: La identidad de usuario 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 del usuario se utiliza para auditar el acceso a dichos sistemas y otros recursos tecnológicos.

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.

Información sensible para el funcionamiento del despacho: Se puede definir como información sensible para un despacho todo lo referente a información privada como claves de usuario para ingresar a los diferentes recursos (red y correo electrónico) de las personas que lo integran así como también datos personales de las colaboradores.

Información pública: Aquella información que permite el adecuado control y manejo de fondos públicos, así como la pertinencia de los servicios públicos que presta el Poder Judicial, al facilitar a las y los administrados, ejercer un control de la legalidad, oportunidad, conveniencia y eficacia de la función administrativa desplegada por la Institución.

Infraestructura Tecnológica: Es el conjunto de todos los dispositivos de hardware y los sistemas o paquetes informáticos, que se utilizan para realizar el trabajo en la institución.

Malware: La palabra es una abreviatura de su nombre en inglés “Malicious Software” la cual comprende todo tipo de virus, spyware, 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.

Plan de Contingencia: Se define como plan de contingencia al conjunto de procedimientos y recursos que tiene la institución como alternativa para lograr mantener el funcionamiento normal de la misma, en caso de que se presente algún incidente interno o externo a la institución.

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.

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.

Red Interna (Intranet): Red Informática privada restringida para el uso de un grupo de personas específico; por ejemplo, usuarios de una organización, de un edificio o de un conjunto de oficinas.

Red Internacional (Internet): Es un conjunto descentralizado de redes de comunicación que permite la comunicación entre diferentes computadores y de sistemas informáticos independientes.

Reglamento: Documento con reglas sobre algún tema. Para el caso de esta normativa, se entenderá como el presente "Reglamento para la administración y uso de los recursos tecnológicos del Poder Judicial".

Riesgo: Es la probabilidad de que una amenaza se materialice y cause un daño o perjuicio.

SGSI: Es un Sistema de Gestión de la Seguridad de la Información, que consiste de una serie de actividades de gestión que deben realizarse mediante procesos sistemáticos, documentados y conocidos por una organización o entidad.

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.

TI: Tecnologías de Información.

Usuarios: Persona tanto interna como externa al Poder Judicial que utiliza cualquier servicio o sistema operativo o bien que tenga acceso a los diferentes recursos tecnológicos del Poder Judicial.

Uso personal: Acciones realizadas por las y los usuarios utilizando los recursos tecnológicos de la institución, en actividades no relacionadas con las funciones asignadas dentro del Poder Judicial.

Capítulo II

Dirección de Tecnología de Información y Comunicaciones.

Artículo 4.- La Dirección de Tecnología de Información y Comunicaciones, en coordinación con la Comisión Gerencial de Tecnologías de la Información, es la responsable de formular y proponer a la Corte Plena, o el órgano que ésta designe, las

políticas en materia tecnológica del Poder Judicial y debe velar por su cumplimiento una vez que se hayan valorado y aprobado.

Artículo 5.- La Dirección de Tecnología de Información y Comunicaciones tiene la responsabilidad de definir los mecanismos que permitan aplicar y verificar el cumplimiento de lo establecido en este reglamento.

Artículo 6.- La Dirección de Tecnología de Información y Comunicaciones es la encargada de desarrollar e implementar aquellos proyectos que hayan sido aprobados por la Corte Plena o el Consejo Superior y cuenten con los recursos presupuestarios y humanos correspondientes.

En materia de tecnología de la información y comunicaciones deberá establecerse un proceso continuo de promulgación y divulgación de un marco estratégico, constituido por políticas organizacionales que sean de fácil comprensión para todo el personal.

Articulo 7.- La Dirección de Tecnología 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 y las posibilidades presupuestarias, manteniendo en todo momento un enfoque de mejora continua.

Artículo 8.- La Dirección de Tecnología de Información y Comunicaciones, previa aprobación de la Administración Superior, 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.

Artículo 9.- La Dirección de Tecnología de Información y Comunicaciones, en conjunto con la Administración Superior, velarán por la implementación de un marco de seguridad de la información, para lo cual deberán:

a. Establecer un marco metodológico que incluya la clasificación de los recursos de TI, según su criticidad, la identificación y evaluación de riesgos, la elaboración e implementación de un plan para el establecimiento de medidas de seguridad, la evaluación periódica del impacto de esas medidas y la ejecución de procesos de concientización y capacitación del personal.

b. Mantener una vigilancia constante sobre todo el marco de seguridad y definir y ejecutar periódicamente acciones para su actualización.

c. Documentar y mantener actualizadas las responsabilidades asociadas al marco de la Seguridad Informática, tanto del personal de la organización, como de terceros relacionados.

Artículo 10.- La Dirección de Tecnología de Información y Comunicaciones y la Administración Superior, deberán velar porque todo el personal de la organización, conozca y esté comprometido con las regulaciones de seguridad y confidencialidad, a fin de evitar el error humano y el uso inapropiado de los recursos tecnológicos. Para esto deberá realizar lo siguiente:

a. Asignar los recursos físicos, humanos y presupuestarios así como velar por la formulación de los marcos jurídicos.

b. Informar y capacitar a los empleados sobre sus responsabilidades en materia de seguridad, confidencialidad y riesgos asociados con el uso de las TI.

c. Implementar mecanismos para vigilar el debido cumplimiento de dichas responsabilidades.

d. Establecer, cuando corresponda, acuerdos de confidencialidad y medidas de seguridad específicas relacionadas con el manejo de la documentación y rescisión de contratos relacionados con TI.

Artículo 11.- La Dirección de Tecnología de Información y Comunicaciones deberá 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; para lograr esto la Dirección de Tecnología deberá:

a. Definir previamente los requerimientos de seguridad que deben ser considerados en la implementación y mantenimiento de software e infraestructura.

b. Contar con procedimientos claramente definidos para el mantenimiento y puesta en producción del software e infraestructura.

c. Mantener un acceso restringido y los controles necesarios sobre los ambientes de desarrollo, mantenimiento y producción.

d. Controlar el acceso a los programas fuente y a los datos de prueba.

e. La Dirección de Tecnología de Información y Comunicaciones debe concientizar en todo momento a los despachos judiciales y oficinas administrativas con el fin de velar por la integridad de la información para que esta sea la correcta y necesaria para realizar las tareas diarias.

Artículo 12.-La Dirección de Tecnología 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. Un plan de continuidad.
b. Un plan de evaluación de riesgos.
c. Documentación sobre la criticidad de los recursos de TI.

Artículo 13.- La Dirección de Tecnología de Información y Comunicaciones es la responsable de gestionar los proyectos netamente tecnológicos. De igual manera, participará en aquellos que aunque no siendo gestionados directamente por la DTIC, utilicen la tecnología de información como elemento estratégico para el cumplimiento de los objetivos del área ejecutante.

Artículo 14.- La Dirección de Tecnología de Información y Comunicaciones debe ajustarse en la medida de las posibilidades a los marcos normativos vigentes, así como a las mejores prácticas, que sean aplicables al gobierno y gestión de TI.

Artículo 15.- La Dirección de Tecnología de Información y Comunicaciones, en conjunto con la Corte Plena o el órgano que esta designe, estarán a cargo de implementar y mantener las Tecnologías de Información necesarias y en relación con el marco estratégico establecido, para lo cual deberán:

 Desarrollar un plan estratégico de tecnologías de información y comunicaciones quinquenal.

 A la Corte Plena o el órgano que esta designe, le corresponde asignar los recursos presupuestarios, físicos y de recursos humanos que se requieran para el cumplimiento de los proyectos estratégicos tecnológicos que se definan y de acuerdo con una priorización institucional de los mismos.

 Adoptar políticas sobre la justificación, autorización y documentación de solicitudes de implementación o mantenimiento de TI.

 Establecer el respaldo claro y explícito para los proyectos de TI tanto del jerarca como de las áreas usuarias.

 Garantizar la participación activa de las unidades o áreas usuarias, las cuales deben tener una asignación clara de responsabilidades y aprobar formalmente las implementaciones realizadas.

 Instaurar líderes de proyecto con una asignación clara, detallada y documentada de su autoridad y responsabilidad.

 Analizar alternativas de solución de acuerdo con criterios técnicos, económicos, operativos y jurídicos, y lineamientos previamente establecidos.

 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.

 Tomar las previsiones correspondientes para garantizar la disponibilidad de los recursos económicos, técnicos y humanos requeridos.

 Formular y ejecutar estrategias de implementación que incluyan todas las medidas para minimizar el riesgo de que los proyectos no logren sus objetivos, no satisfagan los requerimientos o no cumplan con los términos de tiempo y costo preestablecidos.

 Promover la neutralidad tecnológica en los procesos de adquisición de hardware, software y servicios relacionados con las tecnologías de información y comunicaciones.

Artículo 16.- La Dirección de Tecnología 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 Administración Superior. Cualquier necesidad específica que se tenga y que no esté incluida en esta lista, deberá ser aprobada por la Dirección de Tecnología de Información y Comunicaciones conforme a las directrices emitidas por la Administración Superior.

Para estas tareas, deberá respetarse lo siguiente:

 La Dirección de Tecnología 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.

 Desarrollar y aplicar un marco metodológico que guíe los procesos de implementación y considere la definición de requerimientos, los estudios de factibilidad, la elaboración de diseños, la programación y pruebas, el desarrollo de la documentación, la conversión de datos y la puesta en producción, así como también la evaluación post-implantación de la satisfacción de los requerimientos.

 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.

 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.

 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.

 Controlar las distintas versiones de los programas que se generen como parte de su mantenimiento.

Artículo 17.- Todo proyecto que implique desarrollo o implementación de aplicaciones, páginas web o cualquier otro servicio tecnológico, deberá ser revisado por la Dirección de Tecnología de Información y Comunicaciones, 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.

Artículo 18.- La Dirección de Tecnología de Información y Comunicaciones en coordinación con las dependencias que éste designe, serán los responsables de adquirir, administrar, instalar, dar soporte técnico y mantener actualizada la infraestructura tecnológica, además de velar por el buen funcionamiento de la misma en el Poder Judicial.

Artículo 19.- La Dirección de Tecnología de Información y Comunicaciones debe velar por obtener de forma satisfactoria los objetivos contratados a terceros en lo que corresponde a actualizaciones, implementaciones y mantenimiento de la infraestructura tecnológica o aplicaciones. Con el fin de lograr esto se realizar lo siguiente:

a. Establecer una política relativa a la contratación de productos de software e infraestructura.

b. Contar con la debida justificación para contratar a terceros la implementación y mantenimiento de software e infraestructura tecnológica.

c. Establecer un procedimiento o guía para la definición de los “términos de referencia” que incluyan las especificaciones y requisitos o condiciones requeridas o aplicables, así como para la evaluación de ofertas.

d. Establecer, verificar y aprobar formalmente los criterios, términos y conjunto de pruebas de aceptación de lo contratado; sean instalaciones, hardware o software.

e. Implementar un proceso de transferencia tecnológica que minimice la dependencia de la organización respecto de terceros contratados para la implementación y mantenimiento de software e infraestructura tecnológica.

Artículo 20.- La Dirección de Tecnología de Información y Comunicaciones y el personal designado por éste, son los únicos autorizados a remover, cambiar o intercambiar los componentes internos de los recursos tecnológicos y configurar o reconfigurar, programar o reprogramar e instalar o desinstalar programas (software) en los equipos de la Institución.

Artículo 21.- Es responsabilidad de la Dirección de Tecnología 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.

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

Artículo22.- En contra de lo resuelto técnicamente por la Dirección de Tecnologías de la Información, cabrá recurso de revocatoria ante la misma Dirección y de apelación ante el Consejo Superior.

Capítulo III

Instancias de coordinación de los temas de tecnología de información y comunicaciones en el Poder Judicial.

Sección Primera
De los órganos de coordinación.

Artículo 23.- Con el objeto de coordinar y fomentar el uso de las tecnologías de información y comunicaciones en el Poder Judicial, se constituyen los siguientes órganos permanentes:

 Comisión Gerencial de Tecnologías de la Información.

 Subcomité Institucional de Seguridad de la Información.

 Subcomité Institucional de Continuidad de los Servicios Tecnológicos.

Artículo 24.-. La Dirección de Tecnología de la Información dependerá del Consejo Superior.

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.

La Comisión Gerencial de Tecnologías de la Información es un órgano asesor de la Administración Superior.

Los subcomités son grupos de trabajo para áreas específicas, que apoyan la labor de la Comisión Gerencial de Tecnologías de la Información, así como de la Administración Superior.

Artículo 25.- Todas las dependencias que manejan unidades tecnológicas segregadas de la Dirección de Tecnología de la Información, tienen el deber de apegarse a los principios, políticas, marcos, guías, procedimientos e infraestructuras tecnológicas que dicte la Dirección de Tecnología de Información como ente rector en la materia, incluyendo aspectos como modelos y arquitecturas aprobadas; 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.

Sección Segunda
De la Comisión Gerencial de Tecnologías de la Información.

Artículo 26.- La Comisión Gerencial de Tecnologías de la Información (CGTI) será el órgano encargado de elevar las propuestas en temas de Estrategia Organizacional de la Gestión Tecnológica del Poder Judicial a la Administración Superior, una vez que estas sean analizadas y se cuente con el criterio técnico de la Dirección de Tecnología de Información y Comunicaciones.

Artículo27.- La CGTI tendrá como funciones y atribuciones:

◦ La Comisión Gerencial de Tecnologías de la Información, en conjunto con la DTIC deberán, promover el desarrollo institucional 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.

◦ Proponer políticas a la Administración Superior para que constituyan el marco de referencia del accionar de la función tecnológica, a partir de las propuestas que le facilite la DTIC.

◦ Dar seguimiento y apoyo a la gestión tecnológica, así como al presupuesto global institucional en esta materia.

◦ Proponer ante la Administración Superior 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, esto con un previo análisis y aprobación de la DTIC.

◦ Elevar a la Administración Superior las métricas, indicadores y evaluaciones que le facilite la DTIC que permitan medir el impacto estratégico de las tecnologías de la información en la función judicial.

◦ Integrar en un Plan estratégico de las Tecnologías de Información y Comunicaciones, las estrategias, proyectos y planes estratégicos, táctico y operativos en materia tecnológica, y mantener su correcto alineamiento con el plan estratégico institucional.

◦ Velar por una efectiva y oportuna comunicación de la Dirección de Tecnologías de Información y Comunicaciones y la organización en general.

◦ Velar por que las condiciones ambientales donde se encuentran instalados los equipos sean las apropiadas.

◦ Mantener informada a la Administración Superior sobre el avance y los resultados de los proyectos aprobados en el plan estratégico y su impacto.

◦ Aprobar el anteproyecto de presupuesto y el PAOM relacionado con el desarrollo tecnológico institucional de cada año. Así como la planificación de costos del Plan Estratégico de Tecnologías de Información y Comunicaciones.

◦ Cualquier otra función que le sea asignada por la Administración Superior.

Artículo 28.- La Comisión Gerencial de Tecnologías de la Información estará integrada por las siguientes personas:

 La Presidenta o Presidente de la Corte Suprema de Justicia, quien ejercerá el rol de presidir la Comisión. Sin embargo, quien ejerza la presidencia de la Comisión, podrá delegar en otra persona de su elección, este rol.

 Por una Magistrada o Magistrado representante de cada una de las Salas de la Corte Suprema de Justicia.

 Por dos personas integrantes del Consejo Superior.

 Por el Director o Directora del Despacho de la Presidencia.

 Por el Director o Directora de la Dirección de Tecnología de Información.

 Por el Director o Directora Ejecutiva.

 Por la Directora o Director de la Dirección de Planificación.

 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 Tecnología de la Información.

De igual manera, podrá contarse con la participación de representantes del Organismo de Investigación Judicial, de la Defensa Pública, del Ministerio Público, de las diferentes Comisiones del Poder Judicial, y con asesores externos a la organización, cuando la Comisión lo considere necesario. Los invitados tendrán derecho a voz, pero no a voto.

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

Artículo 29.- La Comisión Gerencial de Tecnologías de la Información será coordinada por la Presidenta o Presidente de la Corte Suprema de Justicia, o bien a quien ésta designe.

Artículo 30.- La Comisión Gerencial de Tecnologías de la Información podrá sesionar en forma ordinaria y extraordinaria. Las sesiones ordinarias se realizarán, al menos, una vez al mes, 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 o a solicitud de al menos cuatro de sus integrantes, por medio de la Dirección de Tecnología de la Información y Comunicaciones, cuando la índole de los asuntos sean urgentes, 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.

Artículo 31.- La Comisión Gerencial de Tecnologías de la Información podrá sesionar válidamente con la presencia de al menos cinco de sus miembros, sean éstos 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.

Artículo 32.- De las funciones de la presidenta o del presidente de la CGTI. La CGTI estará a cargo de una presidenta o un presidente, quien dirigirá las sesiones; y para esos efectos tiene las siguientes funciones:

1. Convocar a las sesiones ordinarias y extraordinarias, de forma directa o a través de la Secretaría de la Comisión.

2. Presidir las sesiones de la Comisión.

3. Abrir y cerrar las sesiones. También las podrá suspender, cuando lo considere procedente, por motivos de conveniencia y oportunidad.

4. Dirigir los debates y poner a votación los asuntos.
5. En coordinación con la Secretaría de la Comisión, comunicar los acuerdos a la Administración Superior, así como a las dependencias que corresponda.

6. En coordinación con la Secretaría de la Comisión, llevar el control de la ejecución de los acuerdos.

7. 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, así como actuar como intermediario entre la Corte Plena y la CGTI, para todos aquellos asuntos que le competan.

Artículo 33.-De las funciones del Director o Directora de la DTIC. A la Dirección de Tecnologías de Información, a través de su Director o Directora, le corresponderá asumir un rol preponderante en la sesiones de la Comisión y ejercerá un liderazgo técnico en el análisis, discusión de los asuntos que sean del conocimiento de la Comisión, proponiendo los proyectos que estime pertinentes e informando sobre el avance de su ejecución. Será obligatoria su participación en las sesiones y en caso de que no asista, participará el subdirector o subdirectora de TIC. Le corresponde además elaborar el orden del día de los asuntos que deba conocer la CGTI.

Artículo 34.- 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.

Artículo 35.- 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 Tercera
Del Subcomité Institucional de Seguridad de la Información

Artículo 36.- El Subcomité Institucional de Seguridad de la información será el responsable de asesorar, analizar y emitir recomendaciones dirigidas a la Comisión Gerencial de Tecnologías de la Información y a la Administración Superior, en materia de Seguridad de la Información tanto a nivel lógico como físico. Estas recomendaciones deberán estudiarse en conjunto con la Dirección de Tecnología de Información y Comunicaciones y contar con su debida aprobación.

Artículo 37.- El Subcomité Institucional de Seguridad de la Información estará conformado por las siguientes personas:

◦ La Directora o el Director de Tecnología de Información o la persona que ésta designe.

◦ Un representante de Control Interno con conocimiento en riesgos.

◦ El responsable de Seguridad de la Información de la Dirección de Tecnología.

◦ La Directora o el Director Jurídico. *Ver nota abajo.

 Un representante del Subcomité Institucional de Continuidad de los Servicios Tecnológicos.

Artículo 38.- El Subcomité Institucional de Seguridad de la Información será coordinada por la Directora o el Director de Tecnología de Información o bien por la persona éste designe.

Artículo 39.- El Subcomité Institucional de Seguridad de la Información podrá sesionar válidamente con la presencia de la mitad más uno de sus miembros y los acuerdos serán adoptados por mayoría simple de los presentes. En caso de empate, se someterá nuevamente a votación en la sesión siguiente.

Artículo 40.- El Subcomité Institucional de Seguridad de la información tendrá las siguientes funciones:

◦ Supervisar la implementación de procedimientos y estándares que se desprenden de las políticas de seguridad de la información.

◦ Proponer estrategias y soluciones específicas para la implantación de los controles necesarios para la implementar las políticas de seguridad establecidas y la debida solución de las situaciones de riesgo detectadas.

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

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

◦ Mantener informada a la Comisión Gerencial de Tecnologías de Información 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.

◦ 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.

◦ Velar por el cumplimiento de los controles, implementación y tratamiento de los riesgos de la institución.

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

Sección Cuarta
Del Subcomité Institucional de Continuidad de los Servicios Tecnológicos

Artículo 41.- El Subcomité Institucional de Continuidad de los Servicios Tecnológicos tendrá como objetivo el análisis, propuesta y administración de un plan de continuidad del servicio en el cual se definan las acciones necesarias para responder de forma adecuada ante cualquier incidente que se presente en la institución, desde el momento en que se necesario utilizar la contingencia hasta el momento en que se dé la vuelta a la normalidad de los servicios, de forma que se reduzca al mínimo su impacto sobre las operaciones y servicios del Poder Judicial.

Artículo 42.- El Subcomité Institucional de Continuidad de los Servicios Tecnológicos estará conformado por las siguientes personas:

 Por el Director o Directora Ejecutiva o persona que ésta delegue.

 Por el Director o Directora de la Dirección de Tecnología de Información o persona que ésta delegue.

 Por un miembro de la Unidad de Control Interno.

 Por un miembro del Departamento de Servicios Generales.

 Por un miembro del Departamento de Gestión Humana.

 Por un miembro del Centro de Apoyo en representación de la Judicatura.
 Por un miembro del Ministerio Pública.

 Por un miembro de la Defensa Pública.

 Por un miembro del Organismo de Investigación Judicial.

La Dirección de Tecnología, llevará el control de las actas y de la ejecución de los acuerdos.

Artículo 43.- El Subcomité Institucional de Continuidad de los Servicios Tecnológicos podrá sesionar válidamente con la presencia de la mitad más uno de sus miembros y los acuerdos serán adoptados por mayoría simple de los presentes. En caso de empate, se someterá nuevamente a votación en la sesión siguiente.

Artículo 44.- El Subcomité Institucional de Continuidad de los Servicios Tecnológicos tendrá las siguientes funciones:

1. Identificar los procesos institucionales que sean de importancia estratégica los cuales son clave para el cumplimiento de las metas de la organización.

2. Velar por la generación de un plan de continuidad que este orientado a la puesta de marcha en forma oportuna de los diferentes procesos institucionales y servicios críticos ante cualquier interrupción o desastre.

3. Establecer planes de capacitación para todo el personal involucrado en la aplicación del plan de continuidad de la institución con el fin de que cada persona conozca su rol y tenga claro cuáles son los procedimientos que debe seguir para lograr el éxito en la ejecución del mismo.

4. Velar por que existan mecanismos adecuados de comunicación entre las diferentes dependencias de la institución con el fin de que se proceda como el plan de continuidad lo indique que en caso de presentarse algún tipo de incidente que se pueda determinar cómo crisis.

5. Mantener actualizado el Plan de Continuidad y velar si existe la necesidad de realizar cambios en los elementos que lo afectan, para lo cual se deben realizar revisiones en forma periódica de las políticas, procesos y cualquier otro elemento que se vea involucrado en el mismo.

6. Una vez establecida la declaratoria de desastre por las instancias pertinentes el comité deberá activar los planes de recuperación asociados.

Capítulo IV

De los recursos y servicios tecnológicos.

Sección Primera
Usos de los recursos tecnológicos institucionales.

Artículo 45.- Los servicios y recursos tecnológicos deberán utilizarse únicamente para propósitos laborales. No está permitido el uso éstos para fines personales o comerciales. En el ejercicio de sus facultades, las personas usuarias deben velar por:

a. 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.

b. No interferir con la productividad o el desempeño laboral de las personas servidoras judiciales, así como demás personas usuarias.

c. No afectar de forma negativa el desempeño de los recursos tecnológicos.

d. No violar las disposiciones o políticas institucionales, leyes nacionales o internacionales.

e. No afectar la imagen del Poder Judicial.

Artículo 46.- En cumplimiento de lo que establece la Ley General de Control Interno, las jefaturas de las oficinas deben velar porque las personas usuarias internas al Poder Judicial, utilicen 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 deben tomar las medidas administrativas correspondientes en caso de incumplimiento, 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 Tecnología de Información.

Artículo 47.- 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, Director(a) del OIJ, Fiscal(a) General, Juez(a) coordinador(a) del despacho judicial, Director(a) Ejecutivo (a), Oficina de la Presidencia, o bien en 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 Tecnología.

La aplicación de la autorización estará a cargo de la Dirección de Tecnología 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 de la institución, creará el acceso correspondiente a los servicios autorizados, generando a partir de ese momento la responsabilidad sobre su debido uso.

Artículo 48.- 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 al correo electrónico e Internet, así como a los servicios de red.

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

La responsabilidad sobre el uso indebido de estas credenciales será responsabilidad de la jefatura que aprobó el permiso respectivo y no desactiva o actualiza la condición de la persona usuaria.

Artículo 49.- 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 Tecnología 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.

Artículo 50.- Las jefaturas y/o personas autorizadas por éstas, deberán controlar y registrar el ingreso y salida de los recursos 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 art.67 de este Reglamento.

Artículo 51.- Las jefaturas deberán velar por que toda información que 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 dispositivos anteriormente citados será responsabilidad de la Dirección de Tecnología 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 Tecnología y las áreas tecnológicas autorizadas, y en caso de pérdida, la responsabilidad recaerá sobre las personas encargadas de ejecutar las funciones y la jefatura correspondiente deberá verificar que se cumplan los diferentes controles.

Artículo 52.- El Poder Judicial tendrá la potestad de monitorear mediante los mecanismos que la Dirección de Tecnología de Información y Comunicaciones disponga, el uso de los recursos y servicios tecnológicos, especialmente cuando exista sospecha de que se esté frente a un comportamiento atípico para la seguridad de la información o la continuidad de sus operaciones. 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.

Sección Segunda
Del correo electrónico.

Artículo 53.- 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.

Artículo 54.- 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 usos indebidos que se detecten, las personas usuarias tienen la obligación de reportarlos inmediatamente a su superior para que se inicie con las medidas correspondientes.

Artículo 55.- 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 Tecnología de Información y Comunicaciones será la responsable de definir con base en criterios técnicos el tamaño máximo de los mensajes de correo.

Artículo 56.- No está permitida la utilización de las cuentas de correo del Poder Judicial para el envío de publicidad.

Artículo 57.- En ningún caso se podrá utilizar el servicio de correo electrónico de forma que interfiera con el rendimiento del servicio o con las labores propias del Poder Judicial.

Artículo 58.- 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 destinado para tal fin, cuando por algún motivo se presente un inconveniente que le permita cumplir con lo aquí estipulado.

Sección Tercera
De la Internet suministrada por la institución.

Artículo 59.- Las personas autorizadas para acceder a los servicios de Internet e Intranet, deberán cumplir con lo siguiente:

a. Respetar la privacidad de otros usuarios. 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.

b. 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.

c. Respetar la integridad de los sistemas de computación. Esto significa que ninguna persona usuaria 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.

d. No obtener ni suministrar información a terceros, salvo autorización de las instancias superiores.

e. No dar a conocer códigos de seguridad tales como contraseñas a otras personas, o entorpecer por ningún medio el funcionamiento de los servicios y telecomunicaciones del Poder Judicial.

f. 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 Tecnología de Información y Comunicaciones o las instancias superiores dispongan para salvaguardar la seguridad y el desempeño del personal.

g. No utilizar programas que vulneren la seguridad de los equipos y servidores del Poder Judicial.

h. No dañar o alterar las características técnicas de los servicios tecnológicos provistos por la Dirección de Tecnología de la Información y otras áreas tecnológicas.

i. 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.

Artículo 60.- La Dirección de Tecnología de la Información será la responsable de implementar mecanismos que permitan proteger la información 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 de la información 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 Tecnología de Información y Comunicaciones la solicitud avalada por la jefatura de mayor rango de sus respectivos ámbitos, Director(a) del OIJ, Fiscal(a) General, Juez(a) coordinador(a), Director(a) Ejecutivo (a), Oficina de la presidencia, o bien las personas que éstas deleguen para estos fines.

La Dirección de Tecnología de Información y Comunicaciones analizará la solicitud en términos del impacto a la seguridad de la información 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.

Artículo 61.- Los equipos computacionales (de escritorio, portátiles o laptops, tabletas, teléfonos inteligentes) propiedad de la institución, serán asignados a las personas usuarias con el objetivo de cumplir sus funciones.

Artículo 62.- La persona usuaria tiene la responsabilidad de utilizar adecuadamente el equipo de cómputo y los periféricos que se le asignen, así 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.

Artículo 63.- 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.

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

Artículo 64.- 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.

Artículo 65.- Las personas usuarias a las que se les asigne equipo computacional están en la obligación de informar a La Dirección de Tecnología 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.

Artículo 66.- 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.

Artículo 67.- La persona usuaria que tengan 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 este sufra o por la pérdida de información contenida en el equipo y que no se encuentre debidamente respaldada en los servidores del Poder Judicial.

Artículo 68.- Es responsabilidad del Poder Judicial, asegurar ante las instancias pertinentes, el equipo móvil de su propiedad.

Artículo 69.- 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.

Artículo 70.- 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 Tecnología 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.

Artículo 71.- La Dirección de Tecnología 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, incluyendo los equipos sean institucionales o personales sin la debida autorización por escrito de la Dirección de Tecnología.

Artículo 72.- Para acceder a la red interna es necesario obtener una clave de usuario y una contraseña. Esta clave debe ser conocida solamente por el usuario y es intransferible.

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 Tecnología de Información y Comunicaciones u otras áreas tecnológicas. Si la persona usuaria sospecha que alguien más está haciendo uso de su clave debe reportarlo de inmediato.

Artículo 73.- Ningún usuario 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.

Artículo 74.- Los servicios de impresión institucionales tanto locales como en red deben ser utilizados únicamente para imprimir documentos relacionados con las labores de la oficina. Queda expresamente prohibido su uso para impresiones de carácter personal.

Artículo 75.- 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).

Queda estrictamente prohibido tener imágenes o videos pornográficos, o software ilegal. Con la salvedad de que la naturaleza del trabajo así lo requiera.

Artículo 76.- 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.

Artículo 77.- 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 del usuario (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.

Artículo 78.- Cuando se detecte un uso no aceptable, 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 hará en cuanto se considere que el uso no aceptable se ha suspendido.

La Dirección de Tecnología de Información, 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

Artículo 79.- Todos los programas de software adquiridos por el Poder Judicial, sea por compra, donación o cesión son propiedad de la institución y mantendrán los derechos que la ley de propiedad intelectual le confiera.

Artículo 80.- El software y las aplicaciones que serán instalados en los equipos computacionales propiedad del Poder Judicial serán aquellos que previamente hayan sido estandarizados por la Dirección de Tecnología de Información y Comunicaciones lo cual incluye tanto software libre, software desarrollado internamente, así como el software de pago y para lo cual se dispondrá siempre de las licencias respectivas.

Artículo 81.- No deberá instalarse en los equipos informáticos ningún tipo de software que no se encuentre autorizado por la Dirección de Tecnología de Información y Comunicaciones, ni licenciado por la institución.

La persona usuaria y la jefatura correspondiente, son responsables ante la institución y/o ante terceros, por la instalación y uso de cualquier software no autorizado que haya sido colocado en el equipo computacional.

Artículo 82.- No está permitido desinstalar software, aplicaciones, borrar archivos del sistema o cambiar configuraciones pre-establecidas para los equipos computacionales sin supervisión o consentimiento expreso de la Dirección de Tecnología de Información y Comunicaciones.

Artículo 83.- 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.

Artículo 84.- Toda instalación, desinstalación o traslado de software incluyendo los de "dominio público" o de "distribución libre" desde y hacia un equipo informático, requiere autorización y coordinación previa de la Dirección de Tecnología de Información y Comunicaciones.

Artículo 85.- La Dirección de Tecnología de Información y Comunicaciones, es responsable de realizar revisiones periódicas para asegurar que sólo software con licencia esté instalado en las computadoras de la institución. Producto de esta revisión, podrá iniciar los procedimientos administrativos correspondientes.

Artículo 86.- Las personas usuarias de los sistemas de información, tienen la responsabilidad de mantener actualizada la información y asegurar la completitud de la misma. En los sistemas que se utilice deben completarse todos aquellos campos que se soliciten de forma obligatoria.

Artículo 87.- La Dirección de Tecnología de Información y Comunicaciones o quienes ésta designe, es la responsable del desarrollo de sistemas de información a utilizar en el Poder Judicial.

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 Tecnología.

Capítulo V

De la Seguridad de la Información

Sección Primera
Deberes de la Dirección de Tecnología de ~~la~~ Información y Comunicaciones.

Artículo 88.- La Dirección de Tecnología de Información y Comunicaciones, en conjunto con las instancias correspondientes, 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:

- Definir las necesidades físicas y ambientales donde se instalarán los equipos e infraestructura tecnológica.

- 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).

 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.

Artículo 89.- La Dirección de Tecnología 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.

Artículo 90.- Es responsabilidad de la Dirección de Tecnología de Información y Comunicaciones respetar en todo momento la privacidad de los usuarios y no divulgar información acerca de las cuentas de usuario o del uso que haga del servicio a menos que sea requerido para cumplir con procedimientos legales por orden de un Juez.

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

Artículo 91.- En caso de que la Dirección de Tecnología 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.

Artículo 92.- 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 Tecnología 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 usuario, extensiones de permisos, entre otros, con el fin de gestionar los permisos o cuentas de usuarios respectivas para acceso a los recursos de la red.

Artículo 93.-Las jefaturas deberán solicitar a La Dirección de Tecnología de Información y Comunicaciones, con previa autorización por parte de la jefatura de mayor rango de sus respectivos ámbitos, Director(a), Fiscal(a) General, Juez(a) coordinador(a), Director(a) Ejecutivo, Oficina de la presidencia, 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 la red. 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 que el servicio no este asociado al puesto, deberá el jefe de mayor rango solicitarlo.

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.

Artículo 94.- Las jefaturas, coordinadores o el personal autorizado oficialmente, deberán tener un control cruzado con la Dirección de Tecnología 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 cada funcionario cuenta con su usuario personal y password.

Artículo 95.- Las jefaturas, coordinadores o el personal autorizado oficialmente, deberán comunicar a la Dirección de la Tecnología de Información y Comunicaciones la necesidad de generar usuarios temporales para ingreso a la red institucional y que han de ser utilizados por personas que laboren en forma meritoria. Estos usuarios deben ser generados con una fecha de caducidad dada por la oficina solicitante y con el mínimo de permisos requeridos para llevar a cabo sus funciones diarias.

Es responsabilidad de la jefatura inmediata del despacho donde la persona meritoria laborará, otorgar las credenciales para el uso de los sistemas de información y es su responsabilidad velar por el uso que estas personas hagan de la información y de los recursos tecnológicos.

Sección Tercera
Deberes de las personas usuarias.

Artículo 96.- Las personas usuarias deberán seguir las directrices institucionales que eviten la introducción de malware o la manipulación indebida de la información. Por tanto, cuando se utilice el acceso a Internet, las comunicaciones electrónicas, las memorias re movibles y otros servicios tecnológicos, deberán:

 Utilizar la Internet y los sistemas de comunicación electrónica de acuerdo con las disposiciones que emita la Administración Superior.

 Mantener las condiciones de seguridad de los sistemas, incluyendo la confidencialidad de las palabras claves.

 Ejecutar la revisión de 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.

 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.

 Abstenerse de utilizar o descargar documentos o archivos que no tengan relación alguna con sus labores habituales.

Artículo 97.- Las personas que realicen una labor en el Poder Judicial, indistintamente de la relación laboral que tengan, 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.

Artículo 98.- Las cuentas de usuario asignadas y el uso que se haga de las mismas, se regirá por las siguientes disposiciones:

 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.

 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.

 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.

 Se deberá cambiar la contraseña de acuerdo con las políticas establecidas por la Dirección de Tecnología de Información y Comunicaciones.

Artículo 99.- En toda comunicación electrónica, la persona usuaria deberá mantener los cuidados, profesionalismo y discreción que guarda con los documentos o memorandos impresos.

Las personas servidoras que se desempeñan en la Dirección de Tecnología de la Información y Comunicaciones, deberán firmar un convenio de confidencialidad para proteger la información sensible y crítica que maneja la institución, los que deberá gestionar su jefatura en coordinación con la Dirección Jurídica.

Capítulo VI

De las Prohibiciones y régimen disciplinario.

Artículo 100.- 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.

Artículo 101.- Queda prohibido 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 Tecnología de Información y Comunicaciones.

Artículo 102.- Queda prohibido 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.

Artículo 103.- Queda prohibido conectar electrodomésticos (microondas, radios, coffee makers, refrigeradores, etc.) a los toma corrientes utilizados para los equipos de cómputo.

Artículo 104.- Queda prohibido ejecutar proyectos relacionados con tecnologías de la información sin que hayan pasado por el proceso de evaluación por parte de la Dirección de Tecnología de Información y Comunicaciones y la Comisión Gerencial de Tecnologías de la Información.

Si alguna oficina desea desarrollar un proyecto que involucre tecnologías de la información, debe plantearlo como parte de los ejercicios de formulación presupuestaria, siguiendo los lineamientos establecidos.

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 luego de ser llevados ante el Consejo Superior para su debida aprobación.

Artículo 105.- Es prohibida 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.

Artículo 106.- Se prohíbe 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.

Artículo 107.- No es permitido descargar, ejecutar o copiar programas de software no autorizados y contrarios a las políticas institucionales.

Artículo 108.- Para el envío de correos electrónicos, no se permite a la persona usuaria:

- Asumir la identidad de otra persona, nombres falsos o anónimos.

- Enviar correos que comprometan la imagen del Poder Judicial.

- Enviar correos tipo "cadena" a uno o más destinatarios.

Artículo 109.- Se prohíbe el envío de correos masivos. Se exceptúan de esta prohibición las oficinas expresamente autorizadas para este fin.

Artículo 110.- Se prohíbe 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 del usuario (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.

Artículo 111.- Las demás que establezca y comunique oportunamente la Administración Superior para lograr un mejor uso de los recursos tecnológicos institucionales.

Artículo 112.- Las infracciones al presente reglamento darán motivo para iniciar el correspondiente procedimiento administrativo disciplinario, de conformidad con lo que dispone la Ley Orgánica del Poder Judicial.

Las jefaturas de las oficinas serán las responsables de iniciar el procedimiento disciplinario, de acuerdo a las disposiciones de la Ley Orgánica del Poder Judicial. Si se tratare de un procedimiento disciplinario contra una persona que se desempeña como jefe de oficina, la responsabilidad de iniciar el proceso disciplinario recae sobre su jefatura inmediata.

Capítulo VII

Disposiciones Finales

Artículo 113.- La interpretación y modificaciones al presente reglamento, corresponde a la Corte Suprema de Justicia.

Artículo 114.-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.

Artículo 115.- Se deroga el **Reglamento para la Administración y uso de los recursos informáticos del Poder Judicial**, aprobado por la Corte Plena en la sesión celebrada el 16 de agosto de 2010, artículo XXV. 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.

Artículo 116.- El presente Reglamento rige a partir de su publicación en el *Boletín Judicial*."
San José, 22 de junio de 2017

Licda. Silvia Navarro Romanini
Secretaria General
Corte Suprema de Justicia

Ref.: 659-2017
@mu