



ÓRGANO JUDICIAL CORTE SUPREMA DE JUSTICIA REPÚBLICA DE EL SALVADOR



POLÍTICAS DE TECNOLOGÍA DE LA INFORMACIÓN Y COMUNICACIÓN DEL ÓRGANO JUDICIAL

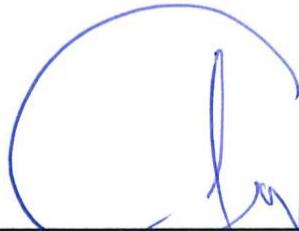
MAYO 2023

	Órgano Judicial Corte Suprema de Justicia Políticas de Tecnología de la Información y Comunicación del Órgano Judicial		PDDTI-02
REVISIÓN 01	Dirección de Desarrollo Tecnológico e Información	MAYO 2023	

“HOJA DE AUTORIZACIÓN Y VIGENCIA”

El presente documento contiene las Políticas de Tecnologías de la Información y Comunicación del Órgano Judicial, preparadas por la Dirección de Desarrollo Tecnológico e Información y revisadas y avaladas por la Gerencia General de Administración y Finanzas, por lo que el **Infrascrito Presidente del Órgano Judicial y de la Corte Suprema de Justicia**, en cumplimiento al Art. 25 de la Ley Orgánica Judicial, **AUTORIZA** las **Políticas de Tecnologías de la Información y Comunicación del Órgano Judicial** y que entrarán en vigencia a partir del **dieciseis de mayo** del año dos mil veintitrés.

Autorizado por:



Lic. Óscar Alberto López Jerez
Presidente del Órgano Judicial y de la Corte Suprema de Justicia



Revisado por:



Lic. José Adalberto Chávez
Gerente General de Administración y Finanzas



Elaborado por:



Ing. Germán Alfonso García García
Director Interino de Desarrollo Tecnológico e Información



	Órgano Judicial Corte Suprema de Justicia Políticas de Tecnología de la Información y Comunicación del Órgano Judicial		PDDTI-02
REVISIÓN 01	Dirección de Desarrollo Tecnológico e Información	MAYO 2023	

INDICE

I. Disposiciones Generales	1
A. Introducción	1
B. Ámbito de aplicación	1
C. Actualizaciones	1
D. Autorización y vigencia	2
E. Principios	2
F. Objetivos	3
Objetivo General	3
Objetivos Específicos	3
G. Marco Legal	3
II. Definiciones	4
III. Políticas de Tecnología de la Información y Comunicación del Órgano Judicial. ..	9
A. Generales	9
B. Administrativas	9
1. Del control e ingreso a las instalaciones de la DDTI	9
a. De aplicación para personal de la DDTI	9
b. De aplicación general	10
2. De la Adquisición de tecnologías de información y comunicaciones	10
3. De las garantías de los equipos y seguro a través de póliza institucional	10
a. De aplicación para personal de la DDTI	10
b. De aplicación general	11
C. Desarrollo, implementación y mantenimiento de sistemas de información.	11
1. Desarrollo de sistemas de información	11
a. De aplicación para personal de la DDTI y personal de Unidades Organizativas que desarrollan funciones similares	11
b. De aplicación general	12
2. Desarrollo de sistemas de información por terceros -outsourcing-	13
a. De aplicación para personal de la DDTI	13
3. Mantenimiento de los sistemas de información	14
a. De aplicación para personal de la DDTI y personal de Unidades Organizativas que desarrollan funciones similares	14
b. De aplicación general	14
4. Control de cambios en Desarrollo de Sistemas de Información	14
a. De aplicación para personal de la DDTI y personal de Unidades Organizativas que desarrollan funciones similares	14

	Órgano Judicial Corte Suprema de Justicia Políticas de Tecnología de la Información y Comunicación del Órgano Judicial		PDDTI-02
REVISIÓN 01	Dirección de Desarrollo Tecnológico e Información	MAYO 2023	

D.	Bases de datos	15
1.	Creación de bases de datos	15
a.	De aplicación para personal de la DDTI y personal de Unidades Organizativas que desarrollan funciones similares	15
2.	Seguridad en bases de datos	15
a.	De aplicación para personal de la DDTI	15
E.	De las redes y telecomunicaciones	16
1.	Redes	16
a.	De aplicación para personal de la DDTI	16
b.	De aplicación general	16
2.	Servicio de Internet y de Correo Electrónico	17
a.	De aplicación para personal de la DDTI	17
b.	De aplicación general	18
F.	Administración del Recurso Informático institucional -hardware y software-	18
1.	Responsabilidades	18
a.	De aplicación para personal de la DDTI	18
b.	De aplicación general	19
2.	Del mantenimiento del <i>hardware</i> institucional	20
a.	De aplicación para personal de la DDTI	20
b.	De aplicación general	20
3.	Licencias de Software	20
a.	De aplicación para personal de la DDTI	20
b.	De aplicación general	21
4.	Instalación de Software	21
a.	De aplicación para personal de la DDTI	21
b.	De aplicación general	22
G.	De la Ciberseguridad	22
1.	Seguridad de acceso a equipos, servidores, sistemas, bases de datos y redes. 22	
a.	De aplicación para personal de la DDTI	22
b.	De aplicación general	23
2.	De la Seguridad Electrónica	25
a.	De aplicación para personal de la DDTI	25
b.	De aplicación general	26
H.	De las copias de respaldo	27
a.	De aplicación para personal de la DDTI	27

	Órgano Judicial Corte Suprema de Justicia Políticas de Tecnología de la Información y Comunicación del Órgano Judicial		PDDTI-02
REVISIÓN 01	Dirección de Desarrollo Tecnológico e Información	MAYO 2023	

- b. De aplicación general 27
- I. Sobre Firma Electrónica..... 27
 - Aspectos Generales 27
 - a. De aplicación para personal de la DDTI..... 28
 - b. De aplicación general 28
- J. Plan de Contingencia y Riesgos Tecnológicos 29
 - a. De aplicación para personal de la DDTI..... 29

	Órgano Judicial Corte Suprema de Justicia Políticas de Tecnología de la Información y Comunicación del Órgano Judicial		PDDTI-02
REVISIÓN 01	Dirección de Desarrollo Tecnológico e Información	MAYO 2023	

I. Disposiciones Generales

A. Introducción

El concepto de gobierno electrónico en los últimos años, ha generado un incremento del uso de las tecnologías de información y de comunicaciones (TIC) en la administración pública, mejorando la eficiencia, eficacia, la transparencia y la rendición de cuentas hacia la sociedad salvadoreña.

Al mismo tiempo, la necesidad de mejorar los procesos judiciales hace imprescindible implementar el uso de las nuevas tecnologías de la información y comunicaciones (TIC), para obtener así un servicio de justicia informatizado acorde a los tiempos actuales. Por lo que es necesario crear políticas para normar el uso de dichas tecnologías dentro de la institución.

Sin embargo, es importante tomar en cuenta la legislación y normativa salvadoreña, específicamente aquellas que permiten utilizar dichas tecnologías, tales como: Ley de Acceso a la Información Pública -artículo 3-, Ley de Procedimientos Administrativos -capítulo III-, Lineamientos de Gestión Documental y Archivos -lineamiento 5, artículos 5,6 y 7-; y artículo 4 del Decreto Legislativo No. 178, de fecha 19 de octubre de 2000, publicado en el Diario Oficial No. 214, Tomo No. 349, de fecha 15 de noviembre de 2000, en el cual le establece la potestad otorgada a la Corte Suprema de Justicia para servicio de los tribunales, de utilizar sistemas electrónicos, ópticos, magnéticos, telemáticos, informáticos y Reglamento para el uso y Control de las Tecnologías de Información y Comunicación en las Entidades del Sector Público; Publicado en el Diario Oficial, Tomo N°404 de fecha, 8 de julio de 2014.

En ese sentido, la Dirección de Desarrollo Tecnológico e Información, quien es la responsable de elaborar, proponer y velar por el cumplimiento de políticas relacionadas a las tecnologías de la información y comunicación, presenta el documento de “Política de la Tecnología de la Información y Comunicación del Órgano Judicial”.

B. Ámbito de aplicación

Las políticas definidas en este documento son de aplicación obligatoria para todos los funcionarios y empleados del Órgano Judicial, cuyas actividades se apoyan en herramientas de Tecnologías de la Información y Comunicaciones. Cada apartado se divide en dos partes: las de fiel cumplimiento para el personal de la Dirección de Desarrollo Tecnológico e Información y las de aplicación general las cuales deben ser acatadas por todos funcionarios y empleados del Órgano Judicial.

C. Actualizaciones

El presente documento de Políticas de Tecnología de la Información y Comunicación deberá ser revisado anualmente y actualizado si fuere necesario, por la Dirección de Desarrollo Tecnológico, encargada de su elaboración. Las actualizaciones deberán ser

	Órgano Judicial Corte Suprema de Justicia Políticas de Tecnología de la Información y Comunicación del Órgano Judicial		PDDTI-02
REVISIÓN 01	Dirección de Desarrollo Tecnológico e Información	MAYO 2023	

autorizadas por el titular o el funcionario en quien este delegue, acorde a lo estipulado en el Artículo 33 de las Normas Técnicas de Control Interno Específicas del Órgano Judicial.

D. Autorización y vigencia

Las Políticas de Tecnología de la Información y Comunicación, serán preparadas por la Dirección de Desarrollo Tecnológico e Información y revisadas por la Gerencia General de Administración y Finanzas, y serán autorizadas por el titular o el funcionario en quien este delegue.

E. Principios

- **Oportunidad**

Que las actividades y servicios se realicen de manera congruente a los tiempos establecidos en las planes, manuales e instructivos elaborados por la Dirección de Desarrollo Tecnológico e Información.

- **Racionalidad del Gasto Público**

Tanto en el uso como en las adquisiciones de recursos informáticos, se haga de manera racional y adecuada, tomando en cuenta el principio de austeridad, sin descuidar el aspecto de calidad en los servicios prestados por el personal en unidades organizativas del Órgano Judicial.

- **Eficiencia Energética**

Que las adquisiciones de recursos informáticos, permitan el ahorro y la eficiencia energética, incorporando tecnología amigable al medio ambiente y que conlleven a la búsqueda o fomento de protección de los recursos naturales y medio ambiente.

- **Responsabilidad**

En la calidad, oportunidad, veracidad, confidencialidad y autenticidad de las información y servicios internos y externos, en materia de tecnología, ofrecidos a los usuarios, funcionarios y empleados del Órgano Judicial.

- **Transparencia**

Los procedimientos y actividades se realicen de forma clara y adecuada, facilitando la rendición de cuentas y abonando a la probidad del Órgano Judicial.

- **Agilidad**

Que las actividades se realicen con prontitud, actuando de manera diligente en los diferentes servicios prestados por la Dirección de Desarrollo Tecnológico e Información, a los funcionarios y empleados; así reduciendo de manera sustancial los tiempos y plazos de los procedimientos administrativos y operativos, logrando una mayor eficacia, eficiencia y efectividad en las actividades administrativas realizadas.

	Órgano Judicial Corte Suprema de Justicia Políticas de Tecnología de la Información y Comunicación del Órgano Judicial		PDDTI-02
REVISIÓN 01	Dirección de Desarrollo Tecnológico e Información	MAYO 2023	

F. Objetivos

Objetivo General

Contar con políticas institucionales que permitan mantener la confiabilidad, disponibilidad e integridad de la información, así como facilitar la optimización de los recursos informáticos y las telecomunicaciones, que son propiedad o se encuentran a disposición del Órgano Judicial, para alcanzar los objetivos y metas institucionales; con la finalidad de satisfacer las necesidades y dar un servicio de administración de justicia eficiente, eficaz y accesible a la población y promover la transparencia, mediante la implementación de una infraestructura basada en la aplicación de nuevas tecnologías de la información y comunicación.

Objetivos Específicos

- Promover el uso de las tecnologías de la información y comunicación -TIC- en el Órgano Judicial, con la finalidad de potenciar el acceso a la justicia y mejorar la eficiencia de la Administración de Justicia.
- Fomentar el uso de las nuevas tecnologías de la información y comunicación con el fin de lograr una justicia más accesible, inclusiva, eficiente y que asegure la igualdad de derechos de todas las personas, ayudándoles hacer valer sus derechos de manera más rápida y sencilla.
- Normar el uso de los recursos tecnológicos de información y comunicación para que estos se administren en forma responsable y apropiada, de conformidad con las disposiciones dadas en este documento y otras de carácter institucional.
- Determinar la infraestructura tecnológica a utilizar a fin de garantizar la viabilidad, continuidad y sustentabilidad de la administración de justicia.
- Potenciar y estandarizar el uso de herramientas tecnológicas y de comunicaciones, ya implementadas o consideradas en planes estratégicos y/o operativos de las Unidades Organizativas que cuentan con Personal con la formación técnica específica.
- Ordenar el desarrollo y mantenimiento de aplicaciones y sistemas informáticos, que son de utilidad para el titular, niveles gerenciales y jefaturas de las unidades organizativas de la institución.

G. Marco Legal

- Ley Especial Contra los Delitos Informáticos y Conexos
- Ley del Servicio Civil
- Ley de Procedimientos Administrativos
- Ley de Acceso a la Información Pública
- Ley de Propiedad Intelectual

	Órgano Judicial Corte Suprema de Justicia Políticas de Tecnología de la Información y Comunicación del Órgano Judicial		PDDTI-02
REVISIÓN 01	Dirección de Desarrollo Tecnológico e Información	MAYO 2023	

- Ley de Firma Electrónica
- Reglamento para el uso y Control de las Tecnologías de Información y Comunicación en las Entidades del Sector Público
- Normas Técnicas de Control Interno Específicas del Órgano Judicial
- Políticas para la Gestión del Correo Electrónico del Órgano Judicial

II. Definiciones

Accesos Remotos Controlados: Los accesos remotos controlados son una forma de acceso a sistemas o dispositivos informáticos desde una ubicación remota, en la que se requiere una conexión segura y controlada para garantizar la privacidad, seguridad y control del acceso.

En los accesos remotos controlados, los usuarios remotos se conectan a los sistemas o dispositivos a través de una conexión encriptada y segura, lo que permite acceder a los recursos y aplicaciones como si estuvieran físicamente en el lugar donde se encuentra el sistema o dispositivo.

Ambiente de Producción: Un ambiente de producción es un entorno informático en el que se ejecutan las aplicaciones y sistemas en producción para brindar servicios a los usuarios finales. Se caracteriza por estar configurado y optimizado para proporcionar el máximo rendimiento y disponibilidad de los servicios a los usuarios.

Aplicaciones Informáticas: Las aplicaciones informáticas son programas de software diseñados para realizar una tarea específica en un sistema informático.

Bienes Intangibles: son activos que no tienen una existencia física, pero que tienen un valor económico debido a los derechos legales o comerciales que representan. Estos activos pueden incluir patentes, marcas registradas, derechos de autor, software, secretos comerciales, licencias, contratos, valor de marca, entre otros. Estos activos pueden ser protegidos por leyes de propiedad intelectual para evitar su uso no autorizado.

Certificado de Firma Electrónica: es un documento electrónico que se utiliza para verificar la identidad de una persona o entidad que está firmando documentos en línea.

Ciberseguridad: se refiere a la protección de los sistemas informáticos y de redes de computadoras de amenazas externas como el malware, el hackeo, el robo de información y otros tipos de ataques. Esto se logra implementando medidas de seguridad como monitoreo, cifrado, autenticación, respaldo de datos, software de seguridad y otros para proteger los sistemas informáticos.

Ciclo de Vida de un Sistema de Información: se define como la metodología tradicional para desarrollar un sistema de información, el cual divide el proceso de desarrollo de sistemas en fases, que deben completarse secuencialmente con una división de las actividades de los usuarios finales y los especialistas de sistemas de información. La definición de un ciclo de vida facilita el control sobre los tiempos en que es necesario aplicar recursos de todo tipo (personal, equipos, suministros, etc.) al proyecto.

	Órgano Judicial Corte Suprema de Justicia Políticas de Tecnología de la Información y Comunicación del Órgano Judicial		PDDTI-02
REVISIÓN 01	Dirección de Desarrollo Tecnológico e Información	MAYO 2023	

DDTI -Dirección de Desarrollo Tecnológico e Información-: siglas denominadas a la dependencia de la institución que tiene bajo cargo las tecnologías de la información y comunicación de la institución.

Digitalización: es un proceso tecnológico que permite, mediante la aplicación de técnicas fotoeléctricas o de escáner, convertir la imagen contenida en un documento en papel en una imagen digital.

Dispositivos de Anunciación: Una unidad que contiene una o más luces indicadoras, disposición alfanumérica, monitor computarizado u otros medios equivalentes sobre los cuales cada indicación provee información del estado acerca de un circuito, condición, sistema, o instalación.

Dispositivos de Detección: Un dispositivo que indica una alarma, emergencia, o condición anormal por métodos audibles, visuales o ambos.

Dispositivos de Control de Acceso: Se trata del dispositivo que efectúa la apertura o permite el paso al usuario, por lo general suelen ser electroimanes, contrachapas o cerraduras eléctricas.

DMZ: siglas denominadas a la frase zona desmilitarizada -conocida también como DMZ, sigla en inglés de *demilitarized zone*-. Este tipo de seguridad se utiliza para cualquiera de la red externa que quiera conectarse ilegalmente a la red interna, la zona desmilitarizada se convierte en un callejón sin salida. La DMZ se usa habitualmente para ubicar servidores que es necesario que sean accedidos desde fuera, como servidores de correo electrónico, web y DNS.

E-Justicia: consiste en el mejoramiento continuo de la administración de justicia, con el apoyo de la tecnológica electrónica, que crea programas automáticos para la solución de conflictos. Se conoce en el mundo con la denominación E Justicia, a la Justicia Electrónica, que incorpora a los procesos judiciales, el expediente electrónico, las audiencias virtuales, y la litigación electrónica.

Fichero Electrónico: permite almacenar de forma electrónica los documentos de una entidad para garantizar su disponibilidad, legibilidad y accesibilidad a largo plazo.

Firma Electrónica: la Ley hace referencia a ella como aquel mecanismo técnico que permite identificar a una persona ante un sistema de información, siempre y cuando dicho mecanismo sea confiable y apropiado.

Gobierno Electrónico: en términos generales se puede mencionar que consiste en una automatización de las respuestas que brinda la administración ante una creciente demanda y exigencia de inmediatez por parte de una sociedad que cada vez se encuentra más informatizada. La aplicación de la informática de gestión por parte de los Estados lleva a lo que los usuarios van a percibir como Gobierno Electrónico.

El concepto de gobierno electrónico incluye todas aquellas actividades que se desarrollan para aumentar la eficacia de la gestión pública basándose en tecnologías informáticas.

	Órgano Judicial Corte Suprema de Justicia Políticas de Tecnología de la Información y Comunicación del Órgano Judicial		PDDTI-02
REVISIÓN 01	Dirección de Desarrollo Tecnológico e Información	MAYO 2023	

Gestión Documental o Gestión de Documentos: es el conjunto de normas técnicas y prácticas usadas para administrar los documentos de todo tipo, recibidos y creados en una organización, facilitar la recuperación de información desde ellos, determinar el tiempo que los documentos deben guardarse, eliminar los que ya no sirven y asegurar la conservación a largo plazo de los documentos más valiosos, aplicando principios de racionalización y economía.

HW: siglas utilizadas para la palabra *Hardware*. El cual es utilizado para aludir a los componentes de carácter material que conforman un equipo de computación.

Llaves Biométricas: son dispositivos de seguridad que utilizan características físicas o comportamentales únicas de un individuo para autenticar su identidad. Estas características pueden incluir huellas dactilares, escaneo de retina, reconocimiento facial, voz o patrones de pulsación del teclado. Las llaves biométricas proporcionan un nivel adicional de seguridad y autenticación en comparación con las contraseñas y los PIN tradicionales, ya que son mucho más difíciles de falsificar o robar.

Malware: es un término general que se utiliza para describir cualquier tipo de software malicioso que se utiliza para dañar o infiltrarse en sistemas informáticos sin el conocimiento o consentimiento del usuario. El malware puede incluir virus informáticos, gusanos, troyanos, ransomware, spyware y otros tipos de software malicioso. El malware puede ser distribuido a través de correos electrónicos fraudulentos, descargas de software no confiable, sitios web comprometidos y otras fuentes.

Obsolescencia: equipos, máquinas, dispositivos, software, no funcionales para la institución por carecer de los requerimientos técnicos mínimos para su uso dentro de la infraestructura tecnológica institucional.

Operadores de Registro: son entidades autorizadas para emitir certificados digitales utilizados en la creación de firmas electrónicas y otros procesos de autenticación en línea. Estos operadores de registro son responsables de verificar la identidad de las personas o entidades que solicitan un certificado digital y de garantizar la validez y autenticidad de la firma electrónica asociada.

Outsourcing: también conocido como subcontratación, tercerización o externalización, es el proceso mediante el cual una empresa contrata a otra empresa o individuo externo para realizar una función o tarea específica.

Pista de Auditoría (huellas de auditoría): Consiste en la serie de documentos, archivos informáticos, y otros elementos de información que se examinan durante una auditoría, y muestran cómo las transacciones son manejadas de principio a fin. La presencia de pistas de auditorías fiables y fáciles de seguir es un indicador del buen control interno establecido y constituye la base de la objetividad.

Proceso: es una secuencia de pasos dispuesta con algún tipo de lógica que se enfoca en lograr algún resultado específico.

	Órgano Judicial Corte Suprema de Justicia Políticas de Tecnología de la Información y Comunicación del Órgano Judicial		PDDTI-02
REVISIÓN 01	Dirección de Desarrollo Tecnológico e Información	MAYO 2023	

Proxy: también conocido como servidor proxy, es un servidor intermedio que actúa como intermediario entre los dispositivos de los usuarios y los servidores de destino en Internet. Cuando un usuario solicita un recurso en línea, como una página web o un archivo, el proxy actúa como un filtro que intercepta la solicitud y la reenvía al servidor de destino. En el proceso, el proxy puede modificar la solicitud, agregar información adicional o incluso bloquear el acceso a ciertos recursos. Los proxies pueden ser utilizados para mejorar la privacidad y la seguridad en línea, ya que pueden ocultar la dirección IP del usuario y protegerlo de ataques informáticos. También se pueden utilizar para acelerar la navegación web, ya que pueden almacenar en caché páginas web populares y entregarlas más rápidamente a los usuarios que las soliciten.

Respaldo de la Información Completa: Considera toda la información almacenada en las bases de datos.

Respaldo de la información incremental: se respaldan los datos creados diariamente.

Respaldo de la información diferencial: se respalda todos los datos ingresados de la semana.

Seguridad Informática: también conocida como ciberseguridad o seguridad de tecnologías de la información, es el área de la informática que se enfoca en la protección de la infraestructura computacional y todo lo relacionado con esta y, especialmente, la información contenida o circulante. Para ello existen una serie de estándares, protocolos, métodos, reglas, herramientas y leyes concebidas para minimizar los posibles riesgos a la infraestructura o a la información. La seguridad informática comprende *software* (bases de datos, metadatos, archivos), *hardware*.

Servicios de Streaming: son plataformas en línea que permiten a los usuarios transmitir contenido multimedia, como películas, programas de televisión, música y podcasts, directamente a sus dispositivos conectados a Internet. Algunos ejemplos populares de servicios de streaming incluyen Netflix, Amazon Prime Video, Spotify y YouTube.

Sistemas de Seguridad Electrónica: Un sistema o parte de un sistema combinado que consiste de componentes y circuitos dispuestos para monitorear o controlar la actividad o acceso a una instalación protegida.

Sistema de Alarma de Prevención de Incendio: sistema o parte de un sistema de combinación constituido por componentes y circuitos dispuestos para monitorear y anunciar el estado de la alarma de incendios o la señal de supervisión de dispositivos de activación e iniciar la respuesta adecuada a tales señales.

Sistema de Video Vigilancia (Circuito Cerrado de Televisión (CCTV): un sistema de video en el cual una señal de video análoga o digital viaja desde la cámara hasta la estación de monitoreo de video en los establecimientos protegidos.

Sistema de Control de Acceso: Monitoreo y control del tráfico en el acceso a un área protegida, mediante la identificación del solicitante para la aprobación de una entrada o salida.

	Órgano Judicial Corte Suprema de Justicia Políticas de Tecnología de la Información y Comunicación del Órgano Judicial		PDDTI-02
REVISIÓN 01	Dirección de Desarrollo Tecnológico e Información	MAYO 2023	

Sistema de Información (SI): es un conjunto de elementos orientados al tratamiento y administración de datos e información, organizados y listos para su uso posterior, generados para cubrir una necesidad o un objetivo.

SW: siglas utilizadas para la palabra *Software*. Se utiliza para aludir a un programa o conjunto de programas de cómputo, así como datos, procedimientos y pautas que permiten realizar distintas tareas en un sistema informático.

Tecnologías de la Información y Comunicación: también conocidas como TIC, son el conjunto de tecnologías desarrolladas para gestionar información y enviarla de un lugar a otro. Abarcan un abanico de soluciones muy amplio. Incluyen las tecnologías para almacenar información y recuperarla después, enviar y recibir información de un sitio a otro, o procesar información para poder calcular resultados y elaborar informes.

Token Electrónico: también conocido como token de autenticación o token criptográfico, es un dispositivo portátil de alta tecnología o códigos generados en la nube o en la red local por una aplicación específica que genera una clave de forma aleatoria e irreemplazable y su aplicación varía según accesos físicos, lógicos a los diferentes sistemas de la institución.

VPN: son las siglas de “red privada virtual”, un servicio que le ayuda a mantener la privacidad en línea. La cual establece una conexión segura y cifrada entre el computador e Internet y proporciona un túnel privado para sus datos y comunicaciones mientras utiliza las redes públicas.

	Órgano Judicial Corte Suprema de Justicia Políticas de Tecnología de la Información y Comunicación del Órgano Judicial		PDDTI-02
REVISIÓN 01	Dirección de Desarrollo Tecnológico e Información	MAYO 2023	

III. Políticas de Tecnología de la Información y Comunicación del Órgano Judicial.

A. Generales

1. La Dirección de Desarrollo Tecnológico e Información efectuará diagnósticos periódicos de las necesidades y requerimientos tecnológicos de las dependencias del Órgano Judicial y deberá proyectar las mejoras de las tecnologías de información y comunicaciones, considerando los costos de transición, viabilidad, capacidad técnica, instalaciones, riesgos tecnológicos, vida útil y tasas de crecimiento de la infraestructura tecnológica.
2. La Dirección de Desarrollo Tecnológico e Información será la responsable de formular, proponer y consensuar con los entes involucrados en la institución, el proyecto de presupuesto de los fondos a asignar para la gestión de las tecnologías de información y proyectos tecnológicos a desarrollar, de acuerdo a lo estipulado en el documento de “Políticas sobre la adquisición de tecnologías de la información y comunicaciones en el Órgano Judicial”.
3. La Dirección de Desarrollo Tecnológico e Información asistirá y brindará asesoría a la Presidencia, a las diferentes comisiones conformadas por la Corte Plena, a la Gerencia General de Administración y Finanzas y a las diferentes unidades organizativas en lo referente a las Tecnologías de Información y Comunicaciones del Órgano Judicial.
4. La Dirección de Desarrollo Tecnológico e Información establecerá metas a fin de dar cumplimiento al Plan Estratégico Institucional en lo relacionado a la materia de tecnología con el fin de contribuir a la sistematización digital de los procesos establecidos en las unidades organizativas. Así como la infraestructura tecnológica que garantice la viabilidad, continuidad y sustentabilidad de la administración de justicia, como también la estandarización en el uso de herramientas tecnológicas y de comunicaciones.

B. Administrativas

1. Del control e ingreso a las instalaciones de la DDTI

a. De aplicación para personal de la DDTI

5. Las jefaturas de la Dirección de Desarrollo Tecnológico e Información deberán velar por el registro de todo el personal bajo su cargo en el sistema de seguridad implementado para el ingreso a las instalaciones de la Dirección, en las Unidades/Departamental/Regional u oficinas donde exista acceso limitado o restringido.
6. Para el ingreso a las instalaciones de la DDTI, ubicada en el Edificio de Oficinas Jurídicas y Administrativas de la Corte Suprema de Justicia los empleados autorizados de la Dirección de Desarrollo Tecnológico e Información deben

	Órgano Judicial Corte Suprema de Justicia Políticas de Tecnología de la Información y Comunicación del Órgano Judicial		PDDTI-02
REVISIÓN 01	Dirección de Desarrollo Tecnológico e Información	MAYO 2023	

registrarse en el sistema de seguridad implementado ubicado tanto en la puerta primaria como en la secundaria de la Dirección.

7. El ingreso a la Sección de Soporte Técnico (HW-SW) estará limitado al personal autorizado por el Departamento de Servicios Informáticos y Soporte Técnico.

b. De aplicación general

8. Los usuarios externos, funcionarios y empleados del Órgano Judicial podrán ingresar a la recepción de la Dirección de Desarrollo Tecnológico e Información dentro de los horarios establecidos por la institución y en consideración a lo estipulado en el artículo 11, de la Ley de Procedimientos Administrativos, -normas de atención al público-, para efectos de recepcionar o entregar documentos, solicitar servicios o realizar consultas. Asimismo, podrán ingresar al interior de las oficinas cuando un empleado de la DDTI sea el responsable de ingresarlo y los atiende personalmente, manteniendo visibles sus correspondientes gafetes o carnets de identificación.
9. El acceso al Centro de Datos ubicado en el Edificio de Oficinas Administrativas y Jurídicas de la Corte Suprema de Justicia será de carácter restringido. El ingreso de particulares, a dicho lugar, deberá contar con la autorización previa del Departamento de Gestión de Tecnología en Comunicaciones a través de las bitácoras establecidas para tal fin.
10. El Personal interno o externo de la institución autorizado para el ingreso al Centro de Datos, deberá estar siempre acompañado por personal de la DDTI, y realizar el debido registro en las bitácoras correspondientes, portando en todo momento y de manera visible sus correspondientes gafetes y/o carnet de identificación.
11. En los Centros Judiciales como en otras unidades organizativas donde se encuentren equipos de comunicación tecnológica, queda prohibido utilizar dichas áreas como bodegas, áreas de descanso, resguardo de utensilios de limpieza, etc. Esto con la finalidad de proteger dichos equipos y evitar daño y como consecuencia la suspensión de los servicios tecnológicos.

2. De la Adquisición de tecnologías de información y comunicaciones

12. La adquisición de tecnologías de información y comunicaciones se realizará conforme a lo establecido al documento de políticas de inversión de las tecnologías de información y comunicaciones en el Órgano Judicial.

3. De las garantías de los equipos y seguro a través de póliza institucional

a. De aplicación para personal de la DDTI

13. Las jefaturas de la DDTI deben acatar y aplicar el procedimiento establecido por la Dirección de Desarrollo Tecnológico e Información para solicitar la garantía de los

	Órgano Judicial Corte Suprema de Justicia Políticas de Tecnología de la Información y Comunicación del Órgano Judicial		PDDTI-02
REVISIÓN 01	Dirección de Desarrollo Tecnológico e Información	MAYO 2023	

equipos, activación de la póliza de seguros institucional o soportes adquiridos con el fabricante para equipos informáticos. Únicamente se podrán reportar equipos para reclamo de garantías o soporte con el fabricante aquellos que estén vigentes y que cuenten con el respaldo de un reporte técnico debidamente completado por los técnicos de la DDTI de acuerdo a su competencia.

14. La Dirección de Desarrollo Tecnológico e Información, por medio de los Administradores de Contrato, llevará un control de las garantías de los equipos informáticos y velará por que se gestione ante las empresas suministrantes la reparación o sustitución de los mismos, haciendo cumplir los compromisos contractuales.
15. La Dirección de Desarrollo Tecnológico e Información debe gestionar ante el Departamento de Administración de Seguros de la Gerencia General de Administración y Finanzas, la activación de la póliza de seguros de los equipos informáticos, en aquellos casos que cumplan tanto con el tiempo establecido para reportar, con toda la documentación requerida por el Departamento de Administración de Seguros.
16. Los equipos cuya garantía haya vencido, o que no cuenten con soporte del fabricante y no aplique para la gestión de seguros, se procederá a su evaluación a fin de determinar la posibilidad de a ser reparados por el personal técnico de la Dirección de Desarrollo Tecnológico e Información. Podrá además ser enviado a talleres externos especializados o programar su reemplazo en proceso de compra, quedando también condicionado a la factibilidad técnica y presupuestaria.

b. De aplicación general

17. Es responsabilidad de los funcionarios y empleados del Órgano Judicial respetar el sello que identifica tanto el código de activo fijo como la fecha de caducidad de la garantía que viene adherido a los equipos asignados y velar por su conservación.

C. Desarrollo, implementación y mantenimiento de sistemas de información.

1. Desarrollo de sistemas de información

a. De aplicación para personal de la DDTI y personal de Unidades Organizativas que desarrollan funciones similares

18. El desarrollo e implementación de aplicaciones y sistemas informáticos se llevará a cabo en consonancia con el Plan Estratégico Institucional, siguiendo los estándares y metodologías de desarrollo establecidos por la Dirección de Desarrollo Tecnológico e Información.

	Órgano Judicial Corte Suprema de Justicia Políticas de Tecnología de la Información y Comunicación del Órgano Judicial		PDDTI-02
REVISIÓN 01	Dirección de Desarrollo Tecnológico e Información	MAYO 2023	

19. La Dirección de Desarrollo Tecnológico e Información a través del Departamento de Ingeniería de Software coordinará, desarrollará y dará mantenimiento a aplicaciones y sistemas informáticos que el Órgano Judicial requiera, de acuerdo a los recursos humanos, tecnológicos y disponibilidad presupuestaria que se tenga a su disposición para este fin, si fuera requerido.
 20. Para el desarrollo de aplicaciones y sistemas informáticos, se deberá aplicar una metodología enfocada en el ciclo de vida de sistemas de información, análisis del sistema, diseño del sistema, desarrollo de la programación, pruebas al sistema, implementación del sistema, puesta en producción y monitoreo mediante un proceso unificado, para asegurar la adecuada administración y desarrollo
 21. El desarrollo de aplicaciones y sistemas informáticos se hará bajo lo establecido en la política 18 del presente documento y por el personal técnico debidamente autorizado por la Dirección de Desarrollo Tecnológico e Información, para garantizar la estandarización en la metodología de desarrollo implementada por el Departamento de Ingeniería de Software.
 22. Para las aplicaciones y sistemas informáticos desarrollados por la DDTI, outsourcing y donaciones, deberán contar con la separación de ambientes de desarrollo, pruebas, administración y producción, a fin de garantizar la seguridad e integridad de los mismos.
 23. La Dirección de Desarrollo Tecnológico e Información deberá garantizar el buen funcionamiento de las aplicaciones y sistemas informáticos mediante pruebas y corrección de errores, si es necesario, previo a su entrega definitiva.
 24. No se implementará una aplicación o sistema informático en ambiente de producción hasta que se superen las pruebas que garanticen el buen funcionamiento del mismo y cuente con la autorización de la Dirección de Desarrollo Tecnológico e Información.
 25. El personal involucrado en el análisis, desarrollo e implementación de aplicaciones y sistemas informáticos deberá estar sujeto a las cláusulas del acuerdo de confidencialidad establecido por la institución.
 26. Las aplicaciones y sistemas informáticos desarrollados al interior de la institución serán de uso exclusivo del Órgano Judicial; excepto que exista algún convenio de cooperación entre instituciones.
- b. De aplicación general**
27. Las solicitudes de nuevas aplicaciones o sistemas informáticos a desarrollar, deberán ser formalmente presentadas por las unidades organizativas a la Dirección de Desarrollo Tecnológico e Información.

	Órgano Judicial Corte Suprema de Justicia Políticas de Tecnología de la Información y Comunicación del Órgano Judicial		PDDTI-02
REVISIÓN 01	Dirección de Desarrollo Tecnológico e Información	MAYO 2023	

28. Para el desarrollo de aplicaciones o sistemas informáticos de uso generalizado, que impliquen la sistematización de procedimientos de trabajo sustantivos, las unidades organizativas involucradas deberán realizar el proceso de elaboración o actualización de manuales administrativos, con la asistencia técnica de la Dirección de Planificación Institucional, previo al requerimiento de desarrollo.
29. El desarrollo de aplicaciones o sistemas informáticos requiere que los responsables de las diferentes unidades organizativas aseguren que, una vez implementados, sean utilizados por el personal designado. Sin embargo, si éstos detectan que el sistema ya no cumple con los requisitos de la unidad debido a cambios en los procedimientos o su obsolescencia, la unidad solicitante deberá informar a la DDTI para que pueda hacer los ajustes necesarios en el sistema.

2. Desarrollo de sistemas de información por terceros -outsourcing-

a. De aplicación para personal de la DDTI

30. El Órgano Judicial podrá autorizar y gestionar el outsourcing para el desarrollo de aplicaciones y sistemas informáticos, cuando la Dirección de Desarrollo Tecnológico e Información requiera fortalecer o potenciar su capacidad instalada, o no disponga del recurso humano y/o tecnológico necesario para el desarrollo del mismo; además cuando otros factores como el tiempo no lo permitan por el grado de especialización y complejidad de la herramienta y exista disponibilidad presupuestaria para tal fin.
31. El desarrollo de aplicaciones y sistemas informáticos a través de *outsourcing*, deberá cumplir con lo establecido en las políticas 20 y 21 del presente documento.
32. El control y monitoreo del avance de las aplicaciones y sistemas informáticos por *outsourcing* estará bajo la responsabilidad del Departamento de Ingeniería de Software, quien deberá documentar a través de informes técnicos mensuales y presentarlos al despacho de la DDTI.
33. Los sistemas de información desarrollados por *outsourcing*, deberán ser entregados de manera formal y debidamente documentados, incluyendo los entregables de documentación definidos por la Dirección de Desarrollo Tecnológico e Información.
34. Cuando se trate del desarrollo de sistemas de información a través de *outsourcing*, se debe incluir dentro de la parte contractual la capacitación correspondiente a los funcionarios y empleados judiciales sobre el uso y mantenimiento del nuevo sistema de información. La Dirección de Desarrollo Tecnológico e Información debe informar a la Dirección de Adquisiciones y Contrataciones Institucional u Organismo donante sobre su cumplimiento o incumplimiento.
35. Para el desarrollo de proyectos de aplicaciones y sistemas informáticos por *outsourcing*, deberán designarse dos o más funcionarios y empleados del Órgano

	Órgano Judicial Corte Suprema de Justicia Políticas de Tecnología de la Información y Comunicación del Órgano Judicial		PDDTI-02
REVISIÓN 01	Dirección de Desarrollo Tecnológico e Información	MAYO 2023	

Judicial que cumplan las funciones de “contraparte técnica” de la institución, quienes deberán ser profesionales especializados de la Dirección de Desarrollo Tecnológico e Información y del área usuaria del proyecto del sistema.

3. Mantenimiento de los sistemas de información

a. De aplicación para personal de la DDTI y personal de Unidades Organizativas que desarrollan funciones similares

36. La Dirección de Desarrollo Tecnológico e Información evaluará, de forma periódica, las necesidades tecnológicas detectadas por las unidades organizativas a los sistemas o aplicaciones existentes a fin de determinar la factibilidad técnica y el uso de recursos para el desarrollo del mismo.
37. Será considerado como mantenimiento de aplicaciones y sistemas informáticos a todas las acciones que impliquen modificaciones, correcciones, mejoras o adiciones a los sistemas de información previamente desarrollados e implementados, que soliciten los usuarios de las unidades organizativas del Órgano Judicial.
38. La Dirección de Desarrollo Tecnológico e información definirá el procedimiento y las formalidades necesarias que orienten la forma en que serán desarrolladas las actividades de mantenimiento del desarrollo de las aplicaciones y sistemas informáticos de información.

b. De aplicación general

39. Cada encargado o jefe de las unidades organizativas deberá evaluar los sistemas implementados para comprobar su utilidad, funcionalidad y contribución al cumplimiento de los objetivos y planes institucionales, con la finalidad de validarlos o solicitar su adecuación ante la Dirección de Desarrollo Tecnológico e Información.

4. Control de cambios en Desarrollo de Sistemas de Información

a. De aplicación para personal de la DDTI y personal de Unidades Organizativas que desarrollan funciones similares

40. Los encargados del Desarrollo de Sistemas deberán llevar un control de los cambios en el desarrollo de las aplicaciones y sistemas informáticos, identificando los cambios realizados y las mejoras obtenidas. Dicho control debe ser avalado por el Director de Desarrollo Tecnológico e Información o a quien este delegue.
41. Previo a la implementación de cambios, el encargado del Desarrollo de Sistemas debe planificar las pruebas para reducir incidentes y vigilar la correcta aplicación del procedimiento para su implementación, dejando documentado tanto los incidentes como los cambios exitosos.

	Órgano Judicial Corte Suprema de Justicia Políticas de Tecnología de la Información y Comunicación del Órgano Judicial		PDDTI-02
REVISIÓN 01	Dirección de Desarrollo Tecnológico e Información	MAYO 2023	

42. La Dirección de Desarrollo Tecnológico e Información deberá informar a los funcionarios y empleados que son usuarios de las aplicaciones y sistemas informáticos sobre los cambios realizados e implementados.

D. Bases de datos

1. Creación de bases de datos

a. De aplicación para personal de la DDTI y personal de Unidades Organizativas que desarrollan funciones similares

43. La Dirección de Desarrollo Tecnológico e Información será la encargada de coordinar, y diseñar las bases de datos, que utilizarán las aplicaciones y sistemas informáticos que se desarrollen en la Dirección.

44. En la creación de nuevas bases de datos se deberá generar la documentación de soporte necesaria y adecuada, que permita comprender su estructura física y lógica, así como su contenido.

45. En la definición de nomenclatura para las bases de datos transaccionales éstas deberán estar normalizadas, con la finalidad de garantizar la compatibilidad con otras bases de datos institucionales, para facilitar la integración de los sistemas implementados. A fin de evitar en la medida de lo posible, los datos redundantes o repetitivos para el caso de las bases de datos transaccionales.

2. Seguridad en bases de datos

a. De aplicación para personal de la DDTI

46. El Director de Desarrollo Tecnológico e Información a través del Departamento de Ingeniería de Software, deberá velar porque los sistemas informáticos desarrollados en la DDTI o por outsourcing cuenten con huellas de auditoría que registre todos los movimientos que afecten a las bases de datos, así como los mecanismos de control adecuados, que garanticen su seguridad, su integridad y la confidencialidad de la información institucional almacenada en estas.

47. Es responsabilidad del Director de Desarrollo Tecnológico e Información o de quien este delegue, establecer, mantener y aplicar sistemas de respaldos periódicos para las bases de datos en ambientes de producción de los sistemas implementados en las diferentes unidades organizativas del Órgano Judicial, que se encuentren alojadas en el Centro de Datos institucional.

b. De aplicación general

48. La información que se genere con los datos registrados en las bases de datos, es responsabilidad de las jefaturas de las Unidades Organizativas o de quienes estos

	Órgano Judicial Corte Suprema de Justicia Políticas de Tecnología de la Información y Comunicación del Órgano Judicial		PDDTI-02
REVISIÓN 01	Dirección de Desarrollo Tecnológico e Información	MAYO 2023	

deleguen en la administración de las bases de datos en las dependencias del Órgano Judicial que las generen.

E. De las redes y telecomunicaciones

1. Redes

a. De aplicación para personal de la DDTI

49. La Dirección de Desarrollo Tecnológico e Información a través del Departamento de Gestión de Tecnología en Comunicaciones, será la responsable de la adquisición, administración y mejora de la red informática interna de datos de la institución.
50. La Dirección de Desarrollo Tecnológico e Información brindará el acceso controlado en la red informática interna de datos a los funcionarios y empleados del Órgano Judicial, de acuerdo a la naturaleza de sus funciones.
51. La Dirección de Desarrollo Tecnológico e Información monitoreará periódicamente los accesos a la red informática interna mediante herramientas de seguridad y administración de los servicios informáticos proporcionados a funcionarios y empleados del Órgano Judicial.
52. Los equipos electrónicos de gestión, servidores de archivos e infraestructura de la red informática del Órgano Judicial serán instalados, configurados y mantenidos por el Departamento de Gestión de Tecnología en Comunicaciones o por proveedores externos certificados que fuesen contratados por la Institución bajo la supervisión del Departamento en mención.
53. La Dirección de Desarrollo Tecnológico e Información pondrá en funcionamiento herramientas de control que posibiliten detectar, analizar y bloquear accesos no permitidos, que no sean utilizados para propósitos institucionales y que pongan en riesgo la seguridad de los recursos informáticos y atenten contra su desempeño.

b. De aplicación general

54. Las jefaturas de las unidades organizativas del Órgano Judicial podrán solicitar a la DDTI, a través de los mecanismos definidos por esa Dirección, la creación de usuarios en las aplicaciones o en los sistemas informáticos desarrollados e implementados, cuentas de correo electrónico institucional, acceso a navegación por internet, VPN, accesos remotos controlados y otros servicios informáticos para los empleados bajo su cargo que, por la naturaleza de sus funciones, lo necesiten.
55. Los funcionarios y empleados del Órgano Judicial, accederán a la red informática de datos a través del equipo de cómputo asignado por la institución, por medio de un usuario y contraseña o por otros medios electrónicos que garanticen la identidad

	Órgano Judicial Corte Suprema de Justicia Políticas de Tecnología de la Información y Comunicación del Órgano Judicial		PDDTI-02
REVISIÓN 01	Dirección de Desarrollo Tecnológico e Información	MAYO 2023	

de la persona, como llaves biométricos o doble factor de autenticación, según el nivel de importancia de la información a la que se acceda.

56. Los funcionarios y empleados del Órgano Judicial en lo relacionado al uso, manejo y resguardo de contraseñas, deberán cumplir con lo estipulado en el documento de políticas de contraseñas establecido por la DDTI.
57. Todas las operaciones que se efectúen por medio de la red informática institucional serán responsabilidad única de los funcionarios y empleados del Órgano Judicial al que se le asignó el usuario y contraseña o token electrónico relacionado con las mismas.
58. No es permitido a ningún funcionario o empleado judicial, excepto a los técnicos designados en la DDTI, manipular las configuraciones de los componentes activos de la red informática -*switches, routers*, dispositivos inalámbricos, cableado de red- y demás servicios informáticos institucionales utilizados en las unidades organizativas del Órgano Judicial.
59. No está permitido instalar puntos de acceso a redes Wi-Fi que se conecten a la red del Órgano Judicial sin una justificación adecuada para su uso y sin la autorización de la Dirección de Desarrollo Tecnológico e Información. Si se detecta un punto de acceso no autorizado, se desconectará de inmediato de la red informática de la institución y se reportará a las autoridades como una vulneración de seguridad y un riesgo informático.
60. No está permitida la conexión de equipos informáticos con nombres o direcciones no registrados dentro de la red informática institucional.
61. No se permite el empleo de mecanismos para la manipulación de direcciones de la red informática o cualquier otro uso que pueda afectar a la topología o estructura lógica de la red informática institucional.
62. Ningún funcionario o empleado está autorizado a utilizar analizadores del tráfico que circula por la red informática alámbrica e inalámbrica del Órgano Judicial. Igualmente está prohibido utilizar herramientas de rastreo de puertos o que permitan detectar vulnerabilidades. El uso de estas herramientas sólo está permitido a los administradores de la red informática institucional y bajo situaciones especiales -incidentes de seguridad, denuncias de usuarios y demás situaciones que lo justifiquen-.

2. Servicio de Internet y de Correo Electrónico

a. De aplicación para personal de la DDTI

63. Los servicios de Internet serán administrados por la Dirección de Desarrollo Tecnológico e Información.

	Órgano Judicial Corte Suprema de Justicia Políticas de Tecnología de la Información y Comunicación del Órgano Judicial		PDDTI-02
REVISIÓN 01	Dirección de Desarrollo Tecnológico e Información	MAYO 2023	

64. La Dirección de Desarrollo Tecnológico e Información procurará tomar las previsiones del caso para que se bloquee por medio de software especializado, ataques informáticos, archivos con contenido pornográfico, descargas multimedia de entretenimiento u ocio, programas no autorizados de software, acceso a web para servicios de streaming, operaciones criminales y terroristas, minados de criptomonedas u otras operaciones de lucro personal llevado a cabo por empleados usando recursos del Órgano y cualquier otro tipo de información que no guarde estricta relación con el área profesional del funcionario o empleado.
65. El servicio de correo electrónico se regirá conforme lo establecido en el documento de Políticas para la Gestión del Correo Eléctrico del Órgano Judicial.

b. De aplicación general

66. El acceso a los servicios de internet estará disponible para todos los funcionarios y empleados del Órgano Judicial que tengan la autorización debida a través de los formularios establecidos, toda vez que existan las condiciones de infraestructura tecnológica y administrativa, y que no pongan en riesgo la infraestructura tecnológica e información del Órgano Judicial.
67. El uso del servicio de Internet deberá ser exclusivamente para apoyar y facilitar las funciones administrativas, técnicas y jurisdiccionales de la institución. Por lo que debe de utilizarse estrictamente en lo relacionado con el área profesional de trabajo del funcionario o empleado.
68. Los valores de seguridad, configuración de proxy y los certificados de los navegadores o browser no deberán ser cambiados por los funcionarios y empleados, excepto por indicaciones de la Dirección de Desarrollo Tecnológico e Información.
69. Se prohíbe expresamente el acceso, visualización y almacenamiento de pornografía, malware o cualquier otro fichero electrónico en los equipos informáticos y dispositivos móviles institucionales. Así como, el ingreso a cualquier sitio web que vulnere la seguridad de la red e información de la institución.

F. Administración del Recurso Informático institucional -hardware y software-

1. Responsabilidades

a. De aplicación para personal de la DDTI

70. El Departamento de Gestión de Tecnología en Comunicaciones es responsable de velar por el buen uso y cuidado del hardware que se encuentre al interior del Centro de Datos institucional e instalaciones de la DDTI donde se encuentren equipos de comunicación tecnológica.

	Órgano Judicial Corte Suprema de Justicia Políticas de Tecnología de la Información y Comunicación del Órgano Judicial		PDDTI-02
REVISIÓN 01	Dirección de Desarrollo Tecnológico e Información	MAYO 2023	

71. Es responsabilidad del personal técnico de la DDTI trasladar de manera apropiada los equipos informáticos, soluciones de videoconferencia y otros equipos tecnológicos a fin de mantener en óptimas condiciones dichos equipos. De comprobarse lo contrario será sancionado de acuerdo a la normativa vigente aplicable.
72. La Dirección de Desarrollo Tecnológico e Información, por medio de los Administradores de Contrato, velará por hacer cumplir las garantías respectivas de cada uno de los equipos informáticos de acuerdo a lo contratado y a la normativa vigente aplicable.
73. Es responsabilidad de la Dirección de Desarrollo Tecnológico e Información realizar estudios y diagnósticos para determinar los equipos a sustituir, cuando ya no garanticen la funcionalidad y operatividad adecuada.

b. De aplicación general

74. Los equipos informáticos propiedad del Órgano Judicial, tanto los adquiridos con presupuesto del estado o por donación, estarán bajo la responsabilidad del funcionario o empleado a quién se le asigne, conforme a lo establecido en el art. 40 de las Normas Técnicas de Control Interno Específicas del Órgano Judicial vigente.
75. Los recursos informáticos asignados a cada funcionario y empleado del Órgano Judicial son tipificados como herramientas de trabajo; por lo tanto, estarán bajo dominio y control de la unidad organizativa encargada en el Órgano Judicial.
76. Es responsabilidad de los funcionarios y empleados del Órgano Judicial velar por el buen uso de los equipos de cómputo -estaciones de trabajo-, computadores portátiles, *tablets*, agendas electrónicas y demás equipos asignados. Debiendo cuidarlos, mantenerlos limpios y conservarlos en buen estado de funcionamiento.
77. Es responsabilidad de los funcionarios y empleados del Órgano Judicial custodiar los equipos portátiles asignados, por lo que deberá tomar las medidas de seguridad correspondiente dentro y fuera de la institución para evitar el robo o hurto del equipo o información institucional. Debiendo contar con la autorización de la jefatura inmediata cuando sea necesario trasladar los equipos fuera de la institución dada la naturaleza de sus funciones.
78. Es responsabilidad de los funcionarios y empleados del Órgano Judicial mantener los equipos tecnológicos libres de objetos y materiales que puedan poner en riesgo su operación segura y su buen funcionamiento.
79. Las jefaturas de las diferentes unidades organizativas del Órgano Judicial son responsables de gestionar ante la unidad organizativa encargada del registro del activo fijo institucional el descargo de los equipos informáticos asignados, debiendo presentar el respectivo reporte técnico donde se recomienda el descargo del mismo.

	Órgano Judicial Corte Suprema de Justicia Políticas de Tecnología de la Información y Comunicación del Órgano Judicial		PDDTI-02
REVISIÓN 01	Dirección de Desarrollo Tecnológico e Información	MAYO 2023	

2. Del mantenimiento del *hardware* institucional

a. De aplicación para personal de la DDTI

80. Los equipos con tecnologías obsoletas serán sustituidos por la DDTI, de acuerdo a estudio técnico previo y disponibilidad presupuestaria.
81. La gestión de fondos para incorporar en el proyecto de presupuesto de la institución y para la adquisición de repuestos y accesorios informáticos para la reparación de equipos informáticos, será responsabilidad de la Dirección de Desarrollo Tecnológico e Información.
82. El Departamento de Gestión de Tecnología en Comunicaciones de la DDTI es responsable de velar por el mantenimiento del *hardware* que se encuentre al interior del Centro de Datos institucional y de los equipos de comunicación tecnológica ubicados en los Centros Judiciales.
83. La DDTI a través del Departamento de Gestión de Servicios y Soporte Técnico debe elaborar e implementar anualmente un plan de mantenimiento preventivo de los equipos de cómputo del Órgano Judicial, con la debida autorización del Director.
84. El personal técnico de la Dirección de Desarrollo Tecnológico e Información realizará un diagnóstico preliminar, con el objeto de procurar la solución, o en su defecto girar las instrucciones del procedimiento a seguir para su reparación, de lo cual dejará constancia a través de formulario de Hoja de Reporte Técnico.

b. De aplicación general

85. Será responsabilidad de cada funcionario y empleado del Órgano Judicial reportar oportunamente, a través del Centro de Contacto de la DDTI, los incidentes que ocurran con los equipos informáticos asignados, para implementar las acciones respectivas.
86. Los equipos informáticos no podrán ser desmantelados, cambiados, abiertos ni reparados por personal no autorizado por la Dirección de Desarrollo Tecnológico e Información. Asimismo, sus componentes -entiéndase *mouse*, disco duro, teclado, memoria, fuente de poder, tarjeta madre, entre otros- no podrán ser removidos por personal no autorizado por la DDTI y en caso de estar autorizado debe documentar dicho proceso ejecutado.

3. Licencias de Software

a. De aplicación para personal de la DDTI

87. La Dirección de Desarrollo Tecnológico e Información será responsable de consolidar y requerir las licencias de *software* necesario para el funcionamiento de

	Órgano Judicial Corte Suprema de Justicia Políticas de Tecnología de la Información y Comunicación del Órgano Judicial		PDDTI-02
REVISIÓN 01	Dirección de Desarrollo Tecnológico e Información	MAYO 2023	

los equipos informáticos del Órgano Judicial y el desarrollo eficiente de las actividades diarias de los funcionarios y empleados del Órgano Judicial.

88. La Dirección de Desarrollo Tecnológico e Información llevará un registro y control actualizado de las licencias adquiridas e instaladas en los equipos del Órgano Judicial.

89. La Dirección de Desarrollo Tecnológico e Información coordinará con el Departamento de Contabilidad, los registros del software de los equipos informáticos y sistemas automatizados, a fin de dar cumplimiento a la normativa vigente en cuanto a las conciliaciones de bienes intangibles.

b. De aplicación general

90. Todo equipo informático -computadora de escritorio y *laptop*- contará como mínimo con una licencia para el *software* de: sistema operativo, programa de ofimática y de un antivirus. De requerir un *software* adicional especializado para el desarrollo de sus funciones diarias, este deberá ser solicitado ante la Dirección de Desarrollo Tecnológico e Información y bajo ninguna circunstancia se debe instalar *software* sin la licencia respectiva, de lo contrario se procedería a informar a las autoridades superiores y gestionar las sanciones o acciones administrativas correspondientes.

91. La Dirección de Desarrollo Tecnológico e Información, resguardará en un lugar adecuado y seguro los documentos originales de las licencias, bajo ninguna circunstancia el funcionario o empleado deberá quedarse con estas; si fuera el caso que el suministrante se las entregara, estas deberán ser remitidas a la DDTI para su respectivo control y resguardo.

4. Instalación de Software

a. De aplicación para personal de la DDTI

92. La Dirección de Desarrollo Tecnológico e Información resguardará y registrará los medios de instalación originales del *software* propiedad del Órgano Judicial. Así como del préstamo de los mismos a empleados de la DDTI debidamente autorizados.

93. Únicamente la Dirección de Desarrollo Tecnológico e Información, a través de su personal técnico autorizado, podrá realizar las instalaciones de *software* respectivas.

94. La Dirección de Desarrollo Tecnológico e Información deberá llevar un registro del *software* libre instalado por personal técnico de la DDTI en los equipos informáticos propiedad del Órgano Judicial, con las debidas justificaciones para su uso y la debida autorización del Director DDTI.

	Órgano Judicial Corte Suprema de Justicia Políticas de Tecnología de la Información y Comunicación del Órgano Judicial		PDDTI-02
REVISIÓN 01	Dirección de Desarrollo Tecnológico e Información	MAYO 2023	

95. Las jefaturas de la DDTI que cuenten con personal técnico autorizado para la instalación de *software* deberán consultar previamente con el Departamento de Gestión de Servicios y Soporte Técnico sobre el licenciamiento del mismo y en el caso de *software* libre sobre la existencia de la justificación y autorización del mismo.

96. Los distintos *software* utilizados en la administración de los sistemas de seguridad electrónica deberán ser instalados en la infraestructura de servidores institucional.

b. De aplicación general

97. Se prohíbe la instalación de *software* propiedad del Órgano Judicial en equipos que no pertenezcan a la institución y en los casos de convenios de cooperación debe existir una cláusula que así lo permita.

98. Se prohíbe que los usuarios realicen instalaciones de cualquier tipo de *software* en los equipos informáticos institucionales asignados. De requerir un *software* específico debe solicitarse y justificarse ante la Dirección de Desarrollo Tecnológico e Información para que se evalúe la importancia y necesidad de su instalación para beneficio de la institución.

99. La instalación y uso de *software* libre deberá justificarse e informarse ante la Dirección de Desarrollo Tecnológico e Información, el cual deber debe ser instalado y controlado por el personal técnico autorizado de la DDTI.

100. Los funcionarios y empleados del Órgano Judicial deben de acatar las disposiciones de la Dirección de Desarrollo Tecnológico e Información, en cuanto al *software* que puede tener el equipo informático asignado. Serán responsables directo si es detectado en su equipo, un *software* no autorizado, ilegal o “pirateado”, por lo cual debe responder ante las autoridades del Órgano Judicial.

G. De la Ciberseguridad

1. Seguridad de acceso a equipos, servidores, sistemas, bases de datos y redes.

a. De aplicación para personal de la DDTI

101. La Dirección de Desarrollo Tecnológico e Información es la responsable de implementar y mantener la seguridad lógica adecuada en el acceso a los equipos, sistemas operativos, sistemas de información, bases de datos, redes informáticas, que operen en el Órgano Judicial.

102. La Dirección de Desarrollo Tecnológico e Información, a través del Departamento de Gestión de Tecnología en Comunicaciones, realizará, diseñará e implementará la segmentación lógica de tráfico de red para proveer confidencialidad y privacidad a cada unidad organizativa con el fin de delimitar el acceso a recursos compartidos entre dependencias.

	Órgano Judicial Corte Suprema de Justicia Políticas de Tecnología de la Información y Comunicación del Órgano Judicial		PDDTI-02
REVISIÓN 01	Dirección de Desarrollo Tecnológico e Información	MAYO 2023	

103. La Dirección de Desarrollo Tecnológico e Información establecerá los mecanismos adecuados para el control, verificación y monitoreo de cambios en las contraseñas, número de sesiones activas, seguridad lógica, física de todas las actividades relacionadas con el uso de tecnologías de información en las unidades organizativas del Órgano Judicial.
104. La Dirección de Desarrollo Tecnológico e Información, a través de los medios de comunicación institucionales oficiales, velará porque se realice la divulgación del documento de políticas de contraseñas establecido por la DDTI a los empleados del Órgano Judicial que tengan acceso a la red institucional.
105. La Dirección de Desarrollo Tecnológico e Información implementará estrategias para generar claves de acceso o token electrónico con los niveles adecuados de seguridad.
106. La Dirección de Desarrollo Tecnológico e Información aplicará políticas de seguridad y personalizará los accesos a los recursos de red dinámicamente mediante directorio activo, asignando a cada empleado un rol específico en la jerarquía institucional.
107. La Dirección de Desarrollo Tecnológico e Información, implementará medidas de seguridad física y lógica para las redes informáticas institucionales, esquemas de red con DMZ, consolas de antivirus, manteniéndolos actualizados en la red.
108. La Dirección de Desarrollo Tecnológico e Información velará porque el sistema de circuito cerrado de televisión, sistemas de control de acceso, presenten una transmisión de datos segura por medio de una red de comunicación dedicada.
109. La Dirección de Desarrollo Tecnológico e Información velará por la continuidad de los servicios tecnológicos, por lo que de acuerdo a la criticidad de los servicios deberá establecer los tiempos máximos de restablecimiento de los mismos tras la caída de un servicio.
110. La Dirección de Desarrollo Tecnológico e Información aplicará mecanismos de seguridad para el ingreso a las redes inalámbricas institucionales, diferenciando el uso de redes inalámbricas para uso institucional y para invitados externos.

b. De aplicación general

111. Es responsabilidad de las jefaturas de las unidades organizativas del Órgano Judicial y de la Dirección de Talento Humano Institucional notificar por escrito a la Dirección de Desarrollo Tecnológico e Información sobre la contratación, traslado, permuta, renuncia de los empleados bajo su cargo. Esto con el fin de que se creen, inhabiliten, modifiquen o eliminen los privilegios de acceso a equipos informáticos, sistemas y las diferentes plataformas, dominios y dispositivos informáticos correspondientes.

	Órgano Judicial Corte Suprema de Justicia Políticas de Tecnología de la Información y Comunicación del Órgano Judicial		PDDTI-02
REVISIÓN 01	Dirección de Desarrollo Tecnológico e Información	MAYO 2023	

112. Es responsabilidad de los funcionarios y empleados del Órgano Judicial salvaguardar la confidencialidad de la clave de acceso o token electrónica utilizada y abstenerse de facilitarla a terceros por cualquier motivo. No debe anotar las claves de acceso escritas en medios o lugares donde puedan ser visualizadas por terceros -Ej.: monitor, folders, escritorio, entre otros-.
113. Cada funcionario y empleado del Órgano Judicial será responsable de las acciones que se reporten en los equipos y sistemas con clave de acceso. En los casos de sustitución de usuarios, se asignará al sustituto, un nombre de usuario y una clave de acceso transitoria y nunca la correspondiente a la persona sustituida, si es temporal la sustitución.
114. Cuando el funcionario o empleado del Órgano Judicial olvide y/o extravíe su clave de acceso, deberá identificarse como propietario de la cuenta ante la Dirección de Desarrollo Tecnológico e Información para que se le proporcione una nueva y dicha Dirección, llevará control de estas asignaciones de claves nuevas a usuarios activos.
115. Los funcionarios y empleados del Órgano Judicial usarán el equipo de cómputo en labores exclusivamente de trabajo y serán responsables por el uso adecuado de las herramientas tecnológicas asignadas y las compartidas de uso común como impresoras multifuncionales, escáner, entre otros.
116. Los funcionarios y empleados del Órgano Judicial deberán abstenerse de utilizar los recursos informáticos de la institución para realizar actividades de índole personal o con fines lucrativos. Los recursos asignados deberán ser utilizados únicamente para cumplir los objetivos institucionales.
117. Se prohíbe a los funcionarios y empleados del Órgano Judicial, utilizar el equipo de la oficina para descargar de internet: programas, juegos, música, videos, películas, fotos, protectores de pantalla y todo archivo que provenga de fuentes no confiables, en caso de identificarse dichas prácticas se informará a la jefatura y autoridad superior para que implementen las acciones correctivas.
118. Ningún funcionario o empleado del Órgano Judicial está autorizado para almacenar material pornográfico, o de índole criminal u ofensivo en ningún medio de almacenamiento de las computadoras, dispositivos periféricos u otro dispositivo de almacenamiento institucional, mucho menos propagarlo a otros empleados.
119. Los funcionarios y empleados del Órgano Judicial deben velar porque su equipo tenga protección contra fallas de energía eléctrica o reducciones de voltaje. Para ello, deben informar a las jefaturas inmediatas para que gestionen ante la Dirección de Desarrollo Tecnológico e Información la asignación de estos dispositivos de seguridad.
120. Es responsabilidad de los funcionarios y empleados verificar a través del antivirus instalado en los equipos de cómputo asignado que los dispositivos informáticos

	Órgano Judicial Corte Suprema de Justicia Políticas de Tecnología de la Información y Comunicación del Órgano Judicial		PDDTI-02
REVISIÓN 01	Dirección de Desarrollo Tecnológico e Información	MAYO 2023	

externos a conectar estén libres de virus. Para ello, se instruirá al personal sobre el uso del antivirus por el medio de comunicación que la Dirección de Desarrollo Tecnológico e Información considere pertinente.

121. Está prohibido conectar equipos informáticos que no están autorizados por la Dirección de Desarrollo Tecnológico e Información.

122. El titular, los niveles gerenciales y demás jefaturas de la institución, deberán asegurar la correcta administración de la seguridad física y lógica de la información, verificando se establezcan y mantengan controles que permitan que la información cumpla con las características de confidencialidad, integridad, disponibilidad, confiabilidad y cumplimiento legal.

123. Los funcionarios y empleados del Órgano Judicial, están en la obligación de conocer y aplicar la normativa en materia de seguridad de las tecnologías de la Información y las comunicaciones para lograr un cambio favorable en la cultura organizacional.

2. De la Seguridad Electrónica

2.1 Aspectos Generales

a. De aplicación para personal de la DDTI

124. La Dirección de Desarrollo Tecnológico e Información, a través de la Unidad de Planeación y Seguimiento de Proyectos TIC, elaborará estudios y análisis de las diversas peticiones para la adquisición de los diferentes sistemas de seguridad electrónica según disponibilidad presupuestaria.

125. Los sistemas de seguridad electrónica deberán ser analizados para determinar la obsolescencia de los diferentes sistemas, antes de elaborar el requerimiento de adquisición correspondiente.

126. La Dirección de Desarrollo Tecnológico e Información se encargará de establecer las especificaciones técnicas mínimas de los sistemas de seguridad electrónica en el caso de adquisición y mantenimiento de estos.

127. La Dirección de Desarrollo Tecnológico deberá velar porque todos los sistemas de seguridad electrónica posean suministros de energía secundarios concordantes con su diseño y necesidad específica de alimentación de acuerdo a requerimientos del fabricante.

128. Los diversos sistemas de seguridad electrónica deberán de cumplir con especificaciones técnicas mínimas de acuerdo a las nuevas tecnologías de información y comunicación, usos, ubicación de dispositivos interiores y exteriores entre otras y cumpliendo con las normas y estándares establecidos vigentes.

	Órgano Judicial Corte Suprema de Justicia Políticas de Tecnología de la Información y Comunicación del Órgano Judicial		PDDTI-02
REVISIÓN 01	Dirección de Desarrollo Tecnológico e Información	MAYO 2023	

129. Los sistemas de alarma de detección de incendios deberán estar bajo norma NFPA 72 (Código Nacional de Alarmas de Incendio y Señalización) la cual norma la aplicación, la instalación, ubicación, desempeño, inspección, prueba y mantenimiento de dicho sistema con estándares internacionales y esta adoptada por el Código Eléctrico Nacional (NEC).

b. De aplicación general

2.2 De Detección y Alarma de Incendios.

130. Los administradores de Centros Judiciales de las respectivas zonas a nivel nacional, donde se encuentren instalados los sistemas de alarma de detección de incendios, deberán reportar a la Dirección de Desarrollo Tecnológico e Información, antes de realizar cambios de ubicación de dispositivos por remodelación, cambios estructurales u otros motivos. Debido a que estos pueden repercutir en fallos del sistema en general.

131. Los administradores de Centros Judiciales de las respectivas zonas a nivel nacional, donde se encuentren instalados los sistemas de alarma de detección de incendios deberán coordinar con la Dirección de Desarrollo Tecnológico e Información, la realización de por lo menos dos pruebas al año de los dispositivos de detección y anunciación que integran el referido sistema, esto para la verificación de su correcto funcionamiento.

132. Los administradores de Centros Judiciales de las respectivas zonas a nivel nacional, donde se encuentren instalados los sistemas de alarma de detección de incendios, deberán gestionar el servicio de mantenimiento y limpieza, a fin de asegurar la precisión y la fiabilidad de los sensores. Debiendo determinar con el suministrante el tiempo y recomendaciones a seguir después de que se realiza una fumigación para no afectar la sensibilidad de los sensores.

2.3 De Circuito Cerrado de Televisión

133. Los administradores de Centros Judiciales de las respectivas zonas a nivel nacional, donde se encuentren instalados los sistemas de circuito cerrado de televisión, deberán reportar a la Dirección de Desarrollo Tecnológico e Información, antes de realizar cambios de ubicación de dispositivos por remodelación, cambios estructurales u otros motivos. Debido a que estos pueden repercutir en fallos en comunicación, fallos en registro de datos (grabación), fallos en visualización, fallos del sistema en general.

134. Se deberá establecer a cada sistema de circuito cerrado de televisión un mínimo de grabación de tres meses.

	Órgano Judicial Corte Suprema de Justicia Políticas de Tecnología de la Información y Comunicación del Órgano Judicial		PDDTI-02
REVISIÓN 01	Dirección de Desarrollo Tecnológico e Información	MAYO 2023	

2.4 De Controles de Acceso

135. Los administradores de Centros Judiciales de las respectivas zonas a nivel nacional, donde se encuentren instalados los sistemas de control de acceso, deberán gestionar rutinas de limpieza en barreras vehiculares, arcos magnéticos, arcos de detección, rayos x, etc. como mínimo una vez al año.

H. De las copias de respaldo

a. De aplicación para personal de la DDTI

136. Es responsabilidad de la DDTI implementar periódicamente la obtención de copias de respaldo de la Información resguardada en equipos servidores ubicados bajo responsabilidad de la DDTI.

137. La Dirección de Desarrollo Tecnológico e Información deberá realizar dentro de sus rutinas los siguientes tipos de respaldos de información: respaldo completo, respaldo incremental, respaldo diferencial.

138. La Dirección de Desarrollo Tecnológico e Información deberá comprobar la integridad y confiabilidad del sistema utilizado para realizar los respaldos de información.

139. La Dirección de Desarrollo Tecnológico e Información llevará registro de los respaldos de información realizados.

b. De aplicación general

140. Es responsabilidad de los funcionarios y empleados del Órgano Judicial mantener respaldos de la información -back up- que se encuentren almacenada en local en los equipos de cómputo asignados a través de medios magnéticos o en el espacio en la nube proporcionado a través del servicio brindado en la plataforma de correo electrónico institucional.

I. Sobre Firma Electrónica

Aspectos Generales

141. La Corte Suprema de Justicia actuará como Autoridad de Registro dentro de la infraestructura de firma electrónica durante la vigencia de los servicios.

142. La Corte Suprema de Justicia podrá emitir y gestionar certificados electrónicos de conformidad a las prácticas de certificación y las políticas de certificación establecidas por la empresa suministrante del servicio y avaladas por el Ministerio de Economía de El Salvador.

	Órgano Judicial Corte Suprema de Justicia Políticas de Tecnología de la Información y Comunicación del Órgano Judicial		PDDTI-02
REVISIÓN 01	Dirección de Desarrollo Tecnológico e Información	MAYO 2023	

143. La Corte Suprema de Justicia por medio del Titular de la institución, autorizará los operadores de registro que proponga la Dirección de Desarrollo Tecnológico e Información.

144. La Corte Suprema de Justicia designará los funcionarios que podrán utilizar los servicios de firma electrónica y hará del conocimiento a la Dirección de Desarrollo Tecnológico e Información para el registro y autorizaciones correspondientes.

145. La Corte Suprema de Justicia, a través del área designada, deberá informar inmediatamente a la Dirección de Desarrollo Tecnológico e Información sobre aquellos funcionarios que pasen a cumplir funciones en cualquier otra unidad organizativa a la actual o ante su desvinculación con la Institución a fin de solicitar la revocación de los permisos otorgados para el uso de firma electrónica.

a. De aplicación para personal de la DDTI

146. Los operadores de registro designados por la superioridad estarán bajo la estructura organizativa de la Dirección de Desarrollo Tecnológico e Información y serán los responsables de aprobar las solicitudes de emisión de certificados electrónicos a los funcionarios o empleados asignados por la superioridad.

147. Los operadores de registro deberán asistir y recibir las capacitaciones correspondientes a fin de formarse para el cargo.

148. Los operadores de registro deberán llevar un registro de los datos del certificado y realizar las comprobaciones oportunas para identificar y autenticar correctamente a los funcionarios o empleados autorizados.

149. Los operadores de registro deberán ejecutar correctamente los procedimientos de suspensión, revocación, renovación y re-emisión de los certificados acorde a la normativa establecida en la Ley de Firma Electrónica.

150. Los operadores de registro deberán de tratar con confidencialidad todos los datos personales de los funcionarios que utilicen el servicio de firma electrónica

b. De aplicación general

151. Es responsabilidad del funcionario o empleado que haya sido designado para el uso de firma electrónica el uso adecuado del aplicativo a utilizar para la creación de firma.

152. Será responsabilidad del funcionario o empleado con autorización para el uso de firma electrónica hacer un uso correcto de los certificados otorgados, por lo que deberá asegurarse que su uso sea estrictamente para aquellos propósitos institucionales para lo que están autorizados.

	Órgano Judicial Corte Suprema de Justicia Políticas de Tecnología de la Información y Comunicación del Órgano Judicial		PDDTI-02
REVISIÓN 01	Dirección de Desarrollo Tecnológico e Información	MAYO 2023	

153. Será responsabilidad del funcionario o empleado con autorización para el uso de firma electrónica mantener la confidencialidad de las claves de acceso y autenticación de la firma electrónica a emitir. Por lo que deberá reportar a la Dirección de Desarrollo Tecnológico e Información cualquier incidencia de seguridad relacionada con el uso del certificado de firma electrónica.
154. Será responsabilidad del funcionario o empleado con autorización para el uso de firma electrónica notificar a la Dirección de Desarrollo Tecnológico e Información cuando tenga indicios de vulneración de la contraseña para ingreso del aplicativo para el uso de firma y sello electrónico.
155. El uso del certificado de firma electrónica es intransferible, por lo cual queda prohibido ser transferido a terceros.
156. Es responsabilidad del funcionario o empleado con autorización para el uso de firma electrónica guardar copias de respaldo de los documentos firmados electrónicamente y de los certificados.
157. Será responsabilidad del funcionario o empleado con autorización para el uso de firma electrónica cumplir con las leyes y regulaciones aplicables en relación con el uso de firma electrónica.

J. Plan de Contingencia y Riesgos Tecnológicos

a. De aplicación para personal de la DDTI

158. La Dirección de Desarrollo Tecnológico e Información será responsable de realizar análisis de los riesgos potenciales y el impacto que estos puedan causar, a fin de desarrollar estrategias enfocadas a la continuidad operativa para mitigar el alcance de la afectación, garantizando así la disponibilidad de los servicios brindados a la población y un alto nivel de resiliencia.
159. La Dirección de Desarrollo Tecnológico e Información deberá elaborar la matriz de riesgos tecnológicos a través de la metodología adoptada por la institución, considerando los riesgos y amenazas de TIC que afecten de forma parcial o total la operatividad normal de los servicios de la institución.
160. La Dirección de Desarrollo Tecnológico e Información deberá contar con un plan de contingencia autorizado por el Director; acorde a los resultados obtenidos en la matriz de riesgos elaborada y categorizando el tipo de acción a realizar en cuanto a la medición en tiempo para el restablecimiento de las operaciones tecnológicas.
161. La Dirección de Desarrollo Tecnológico e Información deberá coordinar con el Departamento Administración de Seguros de la Gerencia General de Administración y Finanzas, a fin de hacer cumplir la póliza de seguros de los equipos de cómputo y así mitigar el riesgo provocado ante cualquier tipo de contingencia y desastre natural.