



GOBIERNO DE TAMAULIPAS
PODER JUDICIAL

Políticas de Uso de Recursos Tecnológicos Objetivo y Alcance

El objetivo principal de establecer las Políticas de Uso de los Recursos Tecnológicos es generar seguridad en el manejo de la información, equipos y sistemas de información, promover el uso adecuado de los recursos humanos, materiales y activos tecnológicos en el Poder Judicial del Estado, teniendo como finalidad:

- 1. Mantener en buen estado los equipos de hardware utilizados por el personal del Poder Judicial.*
- 2. Garantizar el uso adecuado de los recursos de hardware y software para tareas laborales y operativas.*
- 3. Salvaguardar la información y la protección de la privacidad de los datos almacenados y procesados a través de las y los servidores judiciales.*
- 4. Facilitar la ejecución de las actividades de tecnologías de la información en las diferentes áreas del Poder Judicial.*
- 5. Determinar el correcto uso de los servicios de comunicación institucional (correo electrónico y Comunicación Procesal).*
- 6. Establecer pautas para el mantenimiento regular de hardware y software.*
- 7. Desarrollar capacitación continua a las y los usuarios sobre las mejores prácticas de uso de hardware y software, así como crear cultura sobre la seguridad informática.*
- 8. Mantener la seguridad y las condiciones adecuadas en el centro de datos (SITE).*

Estas políticas se deben apegar a todas y todos los servidores judiciales de los órganos jurisdiccionales y administrativos que interactúan con los recursos tecnológicos del Poder Judicial del Estado de Tamaulipas; Esto incluye, pero no se limita a computadoras, dispositivos móviles, software, redes y sistemas de Gestión Judicial. Este documento es válido tanto en las instalaciones del Poder Judicial del Estado de Tamaulipas como en entornos remotos, garantizando una coherencia en la manera en que se utilizan y protegen los recursos digitales.

1. Uso Apropiado de Hardware y Software

Objetivo

Generar la responsabilidad individual de las y los usuarios en el acceso y el uso adecuado a los recursos tecnológicos, los cuales están restringidos a usuarios autorizados y previene en todo momento el acceso no autorizado.

1.1. Acceso y Autorización

- Las y los usuarios deben de acceder a los sistemas y dispositivos a través de credenciales únicas.
- Es responsabilidad del usuario cambiar regularmente su contraseña de los sistemas de gestión judicial y deben de ser tratadas con carácter confidencial.
- Las y los usuarios no deben de utilizar cuentas personales en los dispositivos y sistemas de la organización.
- Las y los usuarios deben de cerrar sesión en los sistemas y apagar los dispositivos al concluir su día laboral.

1.2. Obligaciones de las y los Usuarios

- El uso de los equipos y dispositivos es única y exclusivamente para funciones laborales dentro del Poder Judicial.
- Las y los usuarios son responsables de cuidar los dispositivos y equipos asignados. Cualquier daño se debe de informar inmediatamente al departamento de Soporte Técnico y Mantenimiento.
- Las y los usuarios deben de permitir y aplicar las actualizaciones de software recomendados por la Dirección de Informática.
- Está prohibido instalar, descargar y/o ejecutar programas o juegos, que no estén relacionados con las actividades laborales.
- No está permitido imprimir documentos personales, ni de personas ajenas al Poder Judicial.
- Los equipos de cómputo deberán tener de fondo de escritorio el “wallpaper” oficial que podrá ser descargado de la página oficial del Poder Judicial.

1.3. Responsabilidades por Incumplimiento de las Políticas

- Las y los usuarios están obligados a dar vista o poner de conocimiento de algún incumplimiento de éstas políticas a la Dirección de Contraloría o de Visitaduría Judicial.
- Las presuntas violaciones e incumplimiento de estas políticas, serán causa de inicio de investigación por parte de las Direcciones de Contraloría y Visitaduría Judicial, de conformidad con el párrafo cuarto, del artículo 110 de la Ley Orgánica del Poder Judicial del Estado.

2. Adquisición y Mantenimiento de Hardware y Software

Objetivo

Garantizar la inversión eficiente, la legalidad y la funcionalidad continua de los activos tecnológicos del Poder Judicial del Estado de Tamaulipas.

2.1. Proceso de Adquisición de Hardware y Software

- Cualquier solicitud de adquisición de hardware o software debe de ir respaldada por un dictamen técnico expedido por la Dirección de Informática.
- Toda necesidad de recursos tecnológicos será evaluada por la Dirección de Informática y sus departamentos especializados.



GOBIERNO DE TAMAULIPAS
PODER JUDICIAL

- Las solicitudes aprobadas estarán sometidas a evaluación presupuestaria y aprobación por parte de la Dirección de Administración.
- El Departamento de Adquisiciones deberá guiarse en las "Normativas de Adquisición de Equipo Informático" (NAEI) al realizar cotizaciones y pedidos. Dichas normativas tendrán vigencia de 1 año. Cualquier propuesta técnica diferente a las NAEI deberá ser revisada y validada por la Dirección de Informática.

2.2. Licencias y Cumplimiento Legal

- El uso de software debe cumplir con las licencias de uso y los derechos de autor correspondientes. La piratería de software y la distribución no autorizada están estrictamente prohibidas.
- Está estrictamente prohibido el uso de los recursos tecnológicos para actividades ilegales, no éticas o inapropiadas.
- Con el fin de prevenir vulnerabilidades de seguridad, las y los usuarios no deben demorar la instalación de parches de seguridad críticos.

2.3. Mantenimiento Preventivo y Correctivo

- Las y los usuarios deben de respetar el programa de mantenimiento propuesto por la Dirección de Informática, el cual incluirá revisiones regulares, limpieza y ajuste de hardware.
- Las y los usuarios son responsables de realizar respaldos regulares de sus datos para asegurar su recuperación en caso de pérdida de información.
- El personal de Soporte Técnico y Mantenimiento está autorizado para eliminar de los equipos: música; programas ejecutables y portables; imágenes personales; material pornográfico; archivos de configuración de instalación; librerías; archivos comprimidos; o cualquier otro material personal no relacionado a cuestiones laborales.

3. Seguridad y Privacidad

Objetivo

Establecer directrices para la protección de la información confidencial y la seguridad de los recursos tecnológicos, así como garantizar la confidencialidad, integridad y disponibilidad de los activos tecnológicos.

3.1. Seguridad Hardware y Software

- Es responsabilidad únicamente del personal que así designe la Dirección de Informática, para el traslado o reubicación de los equipos de cómputo.
- En caso de robo o pérdida de algún dispositivo las y los usuarios son responsables de informar inmediatamente a través de una vía oficial al departamento de Soporte Técnico y Mantenimiento.
- Es responsabilidad de la Dirección de Informática aprobar la instalación de una nueva aplicación y/o software a cualquier equipo de cómputo que esté conectado a la red del Poder Judicial del Estado de Tamaulipas.

3.2. Privacidad de Datos

- *Las y los usuarios solo deben acceder a datos personales de las y los empleados, justiciables u otros individuos si es relevante para sus tareas laborales y cuentan con la autorización adecuada.*
- *Las y los usuarios solo deben de almacenar datos personales en ubicaciones seguras y protegidas, como los Sistemas de Gestión Judicial.*
- *Queda prohibido la consulta o uso de datos personales de las y los servidores judiciales, justiciables u otros individuos para actividades no autorizadas o ilegales.*
- *Las y los usuarios son responsables de informar a la Dirección de Informática inmediatamente a través de una vía oficial cualquier incidente de seguridad o posible violación de datos.*

4. Uso de Dispositivos BYOD (Bring Your Own Device)

Objetivo

Establecer las responsabilidades de las y los empleados al utilizar sus propios dispositivos para fines laborales, manteniendo un equilibrio entre la productividad y la seguridad de la información dentro del Poder Judicial del Estado de Tamaulipas.

- *Es responsabilidad de la Dirección de Informática aprobar los dispositivos personales que se podrán utilizar con fines laborales dentro del Poder Judicial.*
- *Las y los usuarios son responsables de mantener sus dispositivos personales seguros mediante el uso de contraseñas y funciones de bloqueo.*
- *Las y los usuarios deben mantener sus dispositivos actualizados con las últimas versiones de software y parches de seguridad.*
- *Las y los usuarios deben instalar y mantener activas en todo momento las aplicaciones de seguridad, como antivirus y antimalware.*
- *Las y los usuarios podrán acceder a la red del Poder Judicial solo si cumplen con los requisitos de seguridad establecidos en el presente documento.*
- *Las y los usuarios deben manejar los datos personales de las y los empleados, justiciables u otros individuos de manera cuidadosa y respetar las políticas de privacidad de datos establecidas en el presente documento.*
- *Las y los usuarios son responsables de realizar respaldos regulares de sus datos para asegurar su recuperación.*
- *Está prohibido a las y los usuarios intentar acceder a sistemas o datos a los que no estén autorizados.*
- *En caso de la pérdida o robo de un dispositivo BYOD, las y los usuarios deben de informarlo inmediatamente a la Dirección de Informática a través de una vía oficial.*



5. Vías de Comunicación Oficiales

Objetivo

Garantizar la confidencialidad, integridad y eficiencia de las comunicaciones electrónicas dentro del Poder Judicial del Estado de Tamaulipas a través del correo electrónico y comunicación procesal.

- *El correo electrónico oficial y el sistema de comunicación procesal deben utilizarse exclusivamente para fines laborales y actividades relacionadas con el Poder Judicial.*
- *Se asignará cuenta de correo electrónico oficial y del sistema de comunicación procesal a las y los titulares de área y al personal cuyo cargo requiera.*
- *La información de los buzones dentro del correo electrónico oficial y del sistema de comunicación procesal son responsabilidad del usuario.*
- *Las y los usuarios deben comunicarse de manera profesional, evitando lenguaje inapropiado, ofensivo o difamatorio a través de los medios oficiales de comunicación del Poder Judicial.*
- *Queda prohibido utilizar cuentas de correo electrónico personales para tratar asuntos de trabajo o compartir información confidencial.*
- *La distribución de correos electrónicos debe ser aprobada previamente por la Dirección de Informática.*
- *No está permitido el envío de archivos de tipo ejecutable, protector de pantalla, archivos PIF., archivos .COM, y/o equivalentes que puedan ser potencialmente peligrosos o pongan en riesgo la seguridad de los recursos tecnológicos.*
- *El Poder Judicial se reserva el derecho de monitorear y revisar el contenido de correos electrónicos y comunicación procesal para cumplir con regulaciones y políticas internas.*