



GOBIERNO DE TAMAULIPAS
PODER JUDICIAL

ACUERDO GENERAL 12/2024

PÚBLICO EN GENERAL P R E S E N T E.-

En sesión ordinaria celebrada en esta propia fecha, el Pleno del Consejo de la Judicatura del Estado, emitió el siguiente Acuerdo:

Acuerdo General 12/2024 del Pleno del Consejo de la Judicatura del Estado, mediante el cual se aprueban y expiden las “Políticas Internas de la Dirección de Informática”; y,

CONSIDERANDO

PRIMERO.- Que de conformidad con los párrafos segundo y tercero del artículo 100 de la Constitución Política del Estado, la administración, vigilancia y disciplina del Poder Judicial del Estado, con excepción del Pleno del Supremo Tribunal de Justicia, estará a cargo del Consejo de la Judicatura del Estado contando con independencia técnica, de gestión y para emitir sus resoluciones. Que congruente con lo anterior, el artículo 114, apartado B, fracciones XV, XVII y XXVIII de la Constitución Política del Estado, confiere al Consejo de la Judicatura, entre otras atribuciones, elaborar los reglamentos, acuerdos y circulares necesarios para la buena marcha administrativa del Poder Judicial, dentro del ámbito de su competencia, tendientes a mejorar la impartición de justicia; dictar las medidas que estime pertinentes para que la impartición de justicia sea pronta, completa e imparcial; y, las demás facultades y obligaciones que las leyes le otorguen.

SEGUNDO.- Que el precepto 122, en sus fracciones XVI y XVIII, de la Ley Orgánica del Poder Judicial, establece que son atribuciones del Consejo de la Judicatura elaborar reglamentos, acuerdos y circulares necesarios para la buena marcha administrativa del Poder Judicial, así como la de dictar, en Pleno, Comisiones o por conducto de su Presidente, las medidas que se estimen pertinentes para que la impartición de justicia sea pronta, completa e imparcial.

TERCERO.- Que los párrafos séptimo y octavo del artículo 4º de la Constitución Política del Estado de Tamaulipas, refieren que el gobierno digital es una política pública que contribuirá al crecimiento y desarrollo de la Entidad, promoviendo el uso estratégico de las tecnologías de la información y comunicaciones en todos los órganos del Estado, con el fin de mejorar las condiciones y la calidad de vida de los habitantes de Tamaulipas. Haciendo el señalamiento que los tres poderes de gobierno, los organismos autónomos y los gobiernos municipales, fomentarán el uso de las herramientas tecnológicas y trabajo remoto, en aquellos casos en que se justifique plenamente y no se puedan realizar las actividades regulares de forma presencial.

CUARTO.- Que el artículo 148 de la Ley Orgánica del Poder Judicial del Estado de Tamaulipas, refiere que la Dirección de Informática funcionará a través de tres vertientes fundamentales que se encargarán del desarrollo y tecnologías de información, de la operación y el mantenimiento, y la de Internet. Por su parte, el numeral 150 de ese ordenamiento hace referencia que corresponde a esa Dirección, como función esencial, proporcionar el soporte técnico necesario en materia de informática en apoyo a las funciones administrativas y de impartición de justicia, susceptibles de ser sistematizadas y automatizadas mediante equipos electrónicos, a cuyo efecto tendrá las siguientes funciones: I.- Diseñar los programas y sistemas informáticos de apoyo a todas las áreas del Poder Judicial, que permitan su constante desarrollo; II.- Establecer políticas de seguridad sobre información, sistemas y programas informáticos; (...) VII.- Informar acerca de las características

técnicas de los productos o servicios informáticos que se deseen adquirir y, en su caso, aprobar la recepción de los mismos; VIII.- Actualización constante sobre los avances tecnológicos y científicos que convengan y puedan aplicarse en los programas de modernización del Poder Judicial; IX.- Instalar y mantener en adecuado funcionamiento las redes de computadoras en las diferentes áreas del Poder Judicial; y, X.- Diseñar, elaborar y mantener actualizada una página de Internet y los sistemas que se requieran para el caso, que permita consultar las actividades sobre impartición de justicia del Poder Judicial; entre otras.

QUINTO.- Que en fecha veinticuatro de mayo de dos mil veintitrés, se instaló y tomó protesta el Comité de Innovación y Tecnología Judicial, que dentro de las atribuciones con las que cuenta y que fueron establecidas por acuerdo de veinte abril del año pasado, destacando: "I. Proponer al Pleno del Consejo de la Judicatura y, en su caso, a la Comisión que por competencia corresponda, los criterios considerados como buenas prácticas, reglamentos, acuerdos, lineamientos, políticas, bases, estrategias y prioridades institucionales para implementar en aspectos relacionados a la innovación y tecnología judicial; (...) X. Identificar aquellas iniciativas que permitan fortalecer el ámbito jurisdiccional y administrativo, que creen valor en la institución y economícen los procesos internos; (...)."

SEXTO.- Que mediante oficio CITJ/5/2024 de fecha cinco de abril del presente año, la Presidenta del Comité de Innovación y Tecnología Judicial, informa que en la Cuarta Sesión Ordinaria de ese Comité en el presente año, se aprobó un punto de acuerdo, a efecto de proponer a este Órgano Colegiado, para que se aprueben y expidan las Políticas Internas de la Dirección de Informática, con el objetivo de garantizar la eficiencia operativa, la seguridad de la información y el cumplimiento normativo dentro de la Judicatura del Estado.

SEPTIMO.- Que en un entorno tecnológico en constante evolución, la Dirección de Informática juega un papel crucial en el funcionamiento eficiente, confiable y seguro de los sistemas y servicios dentro del Poder Judicial del Estado de Tamaulipas, por tanto, con el fin de buscar asegurar el acceso, la seguridad y el uso responsable de los recursos tecnológicos, así como garantizar un entorno digital confiable y protegido para todos los empleados del Poder Judicial, se estima pertinente aprobar y expedir las Políticas Internas de la Dirección de Informática, en donde se desprendan las siguientes temáticas: Acceso a los Centros de Datos (Sites); uso responsable de los Centros de Datos (Site); servidores; base de datos; seguridad y accesos a sistemas operativos, equipos de red, bases de datos y servidores; Software; mantenimiento; anomalías y recuperación de desastres; y generales.

Por lo anteriormente expuesto, y por estimarse justificada la propuesta que hace la Presidenta del Comité de Innovación y Tecnología Judicial, con apoyo además en lo dispuesto por los artículos 121 y 122, fracciones XVI y XVIII, de la Ley Orgánica del Poder Judicial del Estado, el Pleno del Consejo de la Judicatura, procede a emitir el siguiente:

ACUERDO

ÚNICO.- Se aprueban y expiden las "Políticas Internas de la Dirección de Informática", consistiendo de la siguiente manera:

Políticas Internas de la Dirección de Informática

OBJETIVO

Estas políticas buscan asegurar el acceso, la seguridad y el uso responsable de los recursos tecnológicos, así como garantizar un



GOBIERNO DE TAMAULIPAS
PODER JUDICIAL

entorno digital confiable y protegido para todos los empleados del Poder Judicial.

ACCESO A LOS CENTROS DE DATOS (SITES)

- Todo acceso a los Sites deberá contar con una autorización previa. Todos los usuarios y/o proveedores de servicios deben registrarse a la entrada, antes de acceder y deben notificar su salida del Site.
- El acceso a los Sites tendrá acceso restringido y será controlado con llaves, tarjetas de control de acceso, códigos pin y/o biométricos donde aplique.
- Toda persona que ingrese a algún centro de datos, deberá estar acompañado en todo momento por el Administrador de Bases de datos, el Administrador de Servidores y/o el Director de la Dirección de Informática.
- Solo cuando el personal este previamente autorizado, se permitirá tomar fotos o videos; esta actividad será supervisada en todo momento por personal de la Dirección de Informática.
- Los accesos a los centros de datos incluyendo pasillo deben de estar libre de tránsito en todo momento, no está permitido almacenar cajas, herramientas o cualquier artículo que bloquee estas áreas.
- Todos los Sites deberán contar con sensores de temperatura y extintores.
- No se podrán introducir ni utilizar ninguno de los siguientes materiales en los Centro de datos:
 - Alimentos ni bebidas
 - Materiales inflamables
 - Equipo de grabación no autorizado
 - Explosivos
 - Armas ni municiones
 - Productos químicos
 - Cualquier tipo de droga
 - Artículos electromagnéticos
 - Materiales radioactivos
 - Animales y mascotas
 - Productos derivados del tabaco
 - Equipos no aprobados por la Dirección de Informática

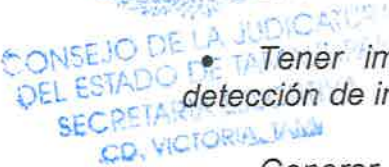
Cualquier otro artículo, sustancia o similar que el Poder Judicial considere como peligroso o dañino.

USO RESPONSABLE DE LOS CENTROS DE DATOS (SITE)

- Los centros de datos no pueden ser utilizados como espacios de almacenamiento de ningún material o artículo ajeno a la operación del mismo.

- Los Sites deben de estar ordenados y limpios en todo momento; se coordinará con el área correspondiente para realizar dicha actividad y será supervisada en todo momento por el Administrador de Bases de Datos o Administrador de Servidores.
- Todo trabajo realizado dentro de un centro de datos será supervisado por el personal que designe la Dirección de Informática; verificando al final que queden ordenados cables, racks, gabinetes y demás componentes que estén en operación.
- Solo con previa autorización se permitirá el uso de aspiradoras, taladros o herramientas de trabajo similares dentro del área de los Sites.
- Se realizará mantenimiento regular a los sistemas de enfriamiento y alimentación eléctrica para garantizar la operación continua del centro de datos.
- Se mantendrá actualizado el registro y seguimiento de cambios en equipos y conexiones en los centros de datos.

SERVIDORES

- 
- 
- Los servidores deben tener instalados los últimos parches de seguridad y sus actualizaciones.
 - El acceso a los servidores es estrictamente para uso laboral.
 - Tener implementados Firewall (cortafuegos) y sistemas de detección de intrusiones en los servidores.
 - Generar un calendario para evaluaciones de vulnerabilidades en los servidores.
 - Está prohibido el uso de los servidores para alojar información, sistemas o sus similares que sean ajenos al Poder Judicial del Estado de Tamaulipas.

BASE DE DATOS

- Son actividades sobre las Bases de Datos que le competen a la Dirección de Informática:
 - Crear, modificar y borrar Bases de Datos.
 - Respalidar Bases de Datos.
 - Recuperar Bases de Datos.
 - Todas las actividades o similares de Administración de Base de Datos que designe el titular de la Dirección de Informática del Poder Judicial.
- Mantener un esquema eficiente para cifrar y respaldar la información de las bases de datos; este proceso debe de ser automatizado con el fin de optimizar recursos.



GOBIERNO DE TAMAULIPAS
PODER JUDICIAL

- Contar con un control de verificación que dichos respaldos se generaron de manera correcta.
- Implementar políticas de acceso basadas en roles para garantizar que solo personal autorizado acceda a los datos.
- La cuenta de acceso es de carácter único y no es transferible.
- Crear los protocolos de auditoría para rastrear el acceso a los datos y detectar actividades inapropiadas.
- Generar un plan de respaldo y almacenamiento seguro de datos en ubicaciones fuera del Site principal.
- Para que el personal ajeno a la Dirección de Informática tenga acceso a las Bases de Datos del Poder Judicial, deberá contar con previa autorización de parte del titular del área.
- Realizar pruebas de restauración a partir de los respaldos generados, a fin de garantizar su correcta generación.
- Identificar claramente el destino de los archivos de respaldo, así como el lugar donde serán reestablecidos con el fin de garantizar un esquema de redundancia.
- Determinar un plan de respaldo completo (data y log de transacciones) diario automatizado al término de la jornada laboral con el fin de minimizar la pérdida de información en una falla general.

SEGURIDAD Y ACCESOS A SISTEMAS OPERATIVOS, EQUIPOS DE RED, BASES DE DATOS Y SERVIDORES

CONSEJO DE LA JUDICATURA
DEL ESTADO DE TAMAULIPAS
SECRETARÍA EJECUTIVA
CD. VICTORIA

- La cuenta de acceso es única, personal e intransferible.
- Los usuarios deben de ser asignados en un esquema de perfiles y/o roles que determinará la Dirección de Informática.
- Ningún usuario podrá contar con permisos de Super Administrador (SA), serán administrados y resguardados por la Dirección de Informática para evitar comprometer la disponibilidad y seguridad de los servicios.
- Las contraseñas deben ser generadas tomando en cuenta las normas vigentes, caracterizándose por ser robustas y sin relación obvia al usuario.
- Se realizarán modificaciones a las claves de seguridad en los siguientes supuestos:
 - Cambio de personal directivo.
 - Cambio de personal en el área de Administrador de Servidores y del Administrador de Bases de Datos
 - Cuando así lo considere la Dirección de Informática
 - Por modificación o re implementación de los sistemas operativos y manejadores de bases de datos.

- Las claves de seguridad serán impresas y guardadas en un sobre sellado, quedando al resguardo de la Dirección de Informática en un lugar seguro.
- Las configuraciones de los equipos de red, deben ser resguardadas por la Dirección de Informática, en una unidad asignada para esta actividad, únicamente tendrá acceso a esta unidad el Director de Informática y el Departamento que éste autorice.
- Las contraseñas de administrador y usuarios de los equipos de cómputo serán generadas y administradas por el Departamento de Soporte Técnico y Mantenimiento, solo tendrá acceso a estas el personal autorizado que designe el Director de Informática.

SOFTWARE

- 
- Generar procesos formales de desarrollo de software, estos deben de incluir diseño, implementación y pruebas.
 - Desarrollar sistemas de información (Gestión Judicial) orientados a satisfacer única y exclusivamente necesidades de las áreas del Poder Judicial.
 - Todo software o aplicación desarrollado por la Dirección de Informática, pasa a ser propiedad del Poder Judicial; solo con autorización previa de la Presidencia es permitido que se comparta.
 - Es responsabilidad del área requirente del desarrollo de software, participar en el análisis y diseño, desarrollo e implementación.
 - Desarrollar manuales de usuario, técnico, de procedimiento y capacitación de cada uno de los desarrollos realizados por la Dirección de Informática.
 - Todo software interno o externo se someterá a pruebas de seguridad y de aceptación antes de su implementación.
 - Respalidar y administrar cada una de las versiones del código fuente de todos los desarrollos que le pertenezcan al Poder Judicial.
 - Establecer políticas de revisión de código para garantizar la calidad y seguridad del software desarrollado.
 - Establecer un proceso formal para solicitar, evaluar y aprobar cambios en sistemas y aplicaciones.
 - Controlar todos los accesos a los sistemas de información (Gestión Judicial).



GOBIERNO DE TAMAULIPAS
PODER JUDICIAL

MANTENIMIENTO

- *Generar cronogramas para el mantenimiento preventivo y documentar los resultados.*
- *Comunicar con anticipación a los usuarios que se verán afectados por el mantenimiento en sistemas y servicios.*
- *Asegurar que las últimas versiones y parches de seguridad estén implementados de manera oportuna en los sistemas operativos, aplicaciones y software.*
- *Llevar a cabo pruebas de continuidad para evaluar la funcionalidad y capacidad de recuperación de los sistemas.*
- *Evaluar y ajustar la capacidad de los recursos tecnológicos según las necesidades del Poder Judicial.*

ANOMALÍAS Y RECUPERACIÓN DE DESASTRES

- *Implementar herramientas de monitoreo para supervisar el rendimiento, la disponibilidad y la salud general en la red, sistemas, aplicaciones y servicios.*
- *Establecer alertas que permitan identificar cualquier anomalía dentro de los recursos tecnológicos del Poder Judicial.*
- *Ante una anomalía actuar de inmediato para investigar la causa y aplicar medidas correctivas; esto puede incluir ajustes en la configuración, actualizaciones de software o intervenciones técnicas.*
- *Implementar un plan detallado de recuperación de desastres que establezca los pasos a seguir en caso de una falla grave.*
- *Realizar pruebas de hackeo ético para evaluar riesgos de seguridad y vulnerabilidades en red, sistemas, aplicaciones y servicios.*
- *Realizar simulacros de recuperación de desastres para evaluar la eficacia de los procedimientos y asegurar que los equipos están preparados para actuar en una situación real de emergencia.*

GENERALES

- *Investigar y evaluar nuevas tecnologías que puedan mejorar la eficiencia del Poder Judicial.*
- *Revisar y actualizar las políticas internas para reflejar los cambios tecnológicos y las necesidades del Poder Judicial.*
- *Garantizar el cumplimiento de regulaciones y estándares relevantes de seguridad y privacidad.*

TRANSITORIOS

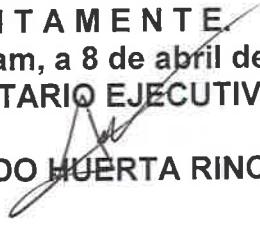
PRIMERO.- El presente acuerdo, surtirá efectos en esta propia fecha.

SEGUNDO.- Se instruye a la Dirección de Informática, a efecto de realizar las gestiones correspondientes.

TERCERO.- Para conocimiento oportuno de las y los interesados, litigantes y público en general, instrúntese el Acuerdo General correspondiente; publíquese en los estrados de la Secretaría Ejecutiva de este Consejo, así como en la página web; asimismo, mediante comunicación procesal a los órganos jurisdiccionales y administrativos de la Judicatura.

Notifíquese.- Así lo acordó el Pleno del Consejo de la Judicatura del Estado, con el voto que por unanimidad emitieron el Magistrado Presidente David Cerda Zúñiga, y Consejeros Ana Verónica Reyes Díaz, Xóchitl Selene Silva Guajardo, José Ángel Walle García y Carlos Ruhneb Pérez Céspedes; quienes firman ante el Secretario Ejecutivo, licenciado Arnoldo Huerta Rincón, que autoriza. Doy fe. SEIS FIRMAS ILEGIBLES. RÚBRICAS.

Lo que se hace de su conocimiento para los efectos legales conducentes.


ATENTAMENTE.
Cd. Victoria, Tam, a 8 de abril de 2024
EL SECRETARIO EJECUTIVO

LIC. ARNOLDO HUERTA RINCÓN
CONSEJO DE LA JUDICATURA
DEL ESTADO DE TAMAULIPAS
SECRETARIA EJECUTIVA
CD. VICTORIA TAM.