CEDETIC

Centro de Desarrollo de Tecnologías de la Información y Comunicaciones

Manual de Políticas

CONTENIDO

INTRODUCCIÓN 4

1. Políticas para usuarios de equipos y sistemas de información del poder judicial del estado 5

1.1. Políticas sobre las responsabilidades de los usuarios de equipos de cómputo en el Poder Judicial 5

1.2 Políticas para el uso de sistemas de información 7

1.3 Políticas sobre el acceso y uso a las redes de voz y datos del Poder Judicial del Estado de Michoacán 7

1.4 Políticas de uso de correo electrónico 8

2. Políticas internas del CEDETIC 9

2.1 Políticas de acceso a los centros de datos (sites) 9

2.2 Políticas de uso de centros de datos (sites) 11

2.3 Políticas de acceso a servidores 12

2.4 Políticas de acceso a bases de datos 13

2.5 Políticas de seguridad en bases de datos 14

2.6 Políticas de seguridad en archivos de datos (información general y anexos) 15

2.7 Políticas de seguridad y manejo de claves de acceso a sistemas operativos, equipos de red y sistemas manejadores de bases de datos .. 16

2.8 Políticas para la videograbación de una audiencia oral 17

2.9 Políticas para el desarrollo de sistemas de información 17

INTRODUCCIÓN

El objetivo principal de establecer las políticas del manejo de la información, equipos y sistemas de información, es promover el uso adecuado de los recursos humanos, materiales y activos tecnológicos en el Poder Judicial del Estado de Michoacán, a través de la definición de lineamientos.

A estos lineamientos se deben apegar los procedimientos y el personal, tanto del CEDETIC, como de todo el resto de las áreas jurisdiccionales y administrativas, en los temas relacionados al uso de equipos y sistemas de información dentro del Poder Judicial del Estado de Michoacán.

Por ello, las políticas buscan específicamente entre otros objetivos los siguientes:

1. Mantener en buen estado los equipos de cómputo utilizados por el personal del Poder Judicial.
2. Asegurar el buen uso de los equipos de cómputo.
3. Asegurar el buen uso de los sistemas de información, en cuanto a la correcta y responsable captura de datos en los mismos, así como el destino adecuado de la información que se obtiene de ellos.
4. Facilitar la ejecución de las actividades de tecnologías de la información en las diferentes áreas del Poder Judicial.
5. Garantizar la seguridad de la información hospedada en los servidores del Poder Judicial.
6. Determinar el correcto uso de los accesos a las bases de datos a fin de evitar mal uso o falla de las mismas.
7. Determinar el correcto uso de los servicios de comunicación institucional (correo electrónico).
8. Mantener la seguridad y las condiciones adecuadas en el centro de datos (SITE).

Políticas para usuarios de equipos y sistemas de información del poder judicial del estado

1.1. Políticas sobre las responsabilidades de los usuarios de equipos de cómputo en el Poder Judicial

- El usuario solo debe de utilizar los equipos de cómputo del Poder Judicial para las funciones laborales.

- No está permitido solicitar al CEDETIC reparaciones o configuraciones de equipos de cómputo personales.

- Los usuarios tienen prohibido instalar, descargar y/o ejecutar programas o juegos, que no sean relacionados con las actividades laborales.

- Los usuarios no deben almacenar 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.

- Del punto anterior, en el caso de que exista ese tipo de información en un equipo, el personal técnico no realizará respaldos en copia de seguridad que la incluya, ni tendrá obligación de recuperarla en el caso de una reinstalación.

- Está prohibido el quitar o desactivar las políticas de restricciones y antivirus.

- El usuario debe de informar al CEDETIC cualquier problema de virus, problema físico o de funcionamiento con su equipo de cómputo.

- El usuario es responsable de cuidar y dar buen uso a su equipo de cómputo.

- El usuario debe cuidar su contraseña personal de computadora, Intranet o cualquier sistema que maneje, no escribirla o mantenerla en algún lugar accesible por otra persona.

- El usuario debe cuidar siempre de bloquear su equipo o cerrar sesión y apagar el equipo cuando lo deje de utilizar.

- El usuario no debe permitir el uso de su equipo oficial a quien no sea personal que labora en el Poder Judicial, salvo los casos donde esté autorizado personal de servicio social, prácticas profesionales o meritorios.

- El usuario debe realizar cambio de sus contraseñas de manera periódica y escogiendo una contraseña segura, siguiendo las recomendaciones que para ello le haga el CEDETIC.

- Toda comunicación o envío de información oficial electrónica debe de hacerse mediante el correo institucional o la Intranet.

- No se debe imprimir documentos personales, ni de personas ajenas a la institución.

- El usuario debe utilizar la impresión en calidad de borrador en las revisiones o documentos no oficiales o importantes, para cuidar los recursos de la Institución.

- No se puede tener acceso a páginas web con fines de ocio, entretenimiento, descargas de archivos, audio y video, o de material pornográfico.

- No se puede modificar el papel tapiz del equipo de cómputo.

- Para todo programa de cómputo o acceso a Internet no autorizado que las áreas requieran, deberán notificar al CEDETIC, quien evaluará, y en

su caso, solicitará autorización al Consejo del Poder Judicial, para su activación o permiso.

- Los equipos portátiles propiedad del Poder Judicial, deberán de contar con una contraseña de arranque que debe de conocer el usuario del equipo, y/o el responsable del área a la cual está asignado el equipo y por el CEDETIC.

1.2 Políticas para el uso de sistemas de información

- El uso de la cuenta de usuario de un sistema de información es responsabilidad de la persona a la que está asignada, es personal e intransferible.

- Todas las contraseñas deberán ser tratadas con carácter confidencial.

- La información que se almacena en un sistema de información es responsabilidad del área que lo utiliza.

- El usuario es responsable de la veracidad, oportunidad y manejo de la información que alimente, y de las consultas que haga de la misma a través del acceso en su sistema.

1.3 Políticas sobre el acceso y uso a las redes de voz y datos del Poder Judicial del Estado de Michoacán

- Solo podrán ser conectados a las redes de datos, los equipos propios del poder judicial, salvo la autorización expresa y con visto bueno por parte del Consejo de Poder Judicial para permitir acceso a equipos ajenos a la Institución.

- Deberán los usuarios sujetarse a los lineamientos de las políticas de uso del Internet y niveles de bloqueo que mediante solicitud del titular le sean asignados.

- Los usuarios deben hacer buen uso del ancho de banda de Internet, absteniéndose de usar redes sociales, sitios de videos o descargas salvo los casos donde por cuestiones de trabajo se requiera.

- Los usuarios deberán de velar por el buen uso y estado que le den a los dispositivos de red, esto es, puntos de acceso, concentradores o ruteadores inalámbricos, así como a las tarjetas inalámbricas y sus antenas, etc. De la misma manera los usuarios no podrán modificar o resetear las configuraciones de los equipos.

- Los usuarios no podrán instalar ningún tipo de programa que sirva para escaneo o monitoreo de red, en caso de encontrarse alguno se notificara de inmediato al Consejo de Poder Judicial.

- El usuario tendrá la obligación de salvaguardar cualquier contraseña de acceso a la red que le sea asignada, así como la responsabilidad del buen uso que este le dé.

1.4 Políticas de uso de correo electrónico

- Se asigna una cuenta oficial de correo electrónico Institucional por cada órgano jurisdiccional o área administrativa. Se asignan cuentas individuales o personales al personal cuyos cargos lo requieren o cuando son solicitadas expresamente para alguna función de trabajo.

- El uso de las cuentas oficiales asignadas al órgano jurisdiccional o área administrativa deben ser administradas por el titular o en su caso delegadas a quien el mismo designe, cuidando el buen uso de la misma.

- El uso del correo electrónico es estrictamente de trabajo.

- No se permiten envíos de correo electrónico masivo para propaganda personal o de otros medios.

- No se permite envió de correo electrónico de cadenas.

- 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 el equipo.

- La información de los buzones es responsabilidad de cada usuario.

- CEDETIC se reserva el derecho de realizar actividades de mantenimiento a los buzones.

- Las cuentas de acceso serán creadas en base al procedimiento de solicitud de cuentas de correo establecido en el Manual de Procedimientos de la Dirección del CEDETIC.

2. Políticas Internas del CEDETIC

2.1 Políticas de acceso a los centros de datos (sites)

- Todo acceso a los centros de datos (sites) del CEDETIC deberán ser autorizados previamente. Se requiere que tanto los usuarios como proveedores de servicios se registren a la entrada, antes de que se les conceda el acceso y notificarse igualmente a su salida del site.

- El acceso a los centros de datos (sites) del CEDETIC estará limitado y será controlado con llaves, o por medio de tarjetas de control de acceso y/o biométricos donde se tengan instalados.

- Cualquier persona con previa autorización de acceso a los centros de datos (sites) del CEDETIC deberá estar acompañado en todo

momento por el Administrador de Bases de datos, el Administrador de Servidores, el Director y/o los Jefes de departamento del CEDETIC.

- No se permiten alimentos ni bebidas dentro de los centros de datos (site) del CEDETIC.

- No se permite tomar fotos ni videos con ningún tipo de dispositivo salvo si el personal cuenta con la autorización correspondiente de la dirección del CEDETIC.

- Toda actividad derivada del punto anterior deberá ser supervisada en todo momento por el Administrador de Bases de datos, el Administrador de Servidores, el Director y/o los Jefes de Departamento del CEDETIC.

- No se deberá bloquear los pasillos o accesos a los centros de datos del CEDETIC, ni almacenar cajas o herramientas en áreas de acceso común al personal autorizado.

- Los usuarios autorizados para el acceso a Centro de datos de CEDETIC (SITE) no pueden introducir ni utilizar ninguno de los siguientes materiales en el Centro de datos:

    - Productos derivados del tabaco
    - Explosivos
    - Armas
    - Químicos
    - Drogas ilegales
    - Artículos electromagnéticos
    - Materiales radioactivos
    - Cámaras fotográficas o de video

- Cualquier otro artículo similar a los antes mencionados, que, a la institución (según políticas), considere como peligrosos o dañinos.

- CEDETIC se reserva el derecho de inspeccionar todos los objetos que entran o salen del Centro de datos.

2.2 Políticas de uso de centros de datos (sites)

- No podrán ser almacenados dentro de ningún espacio en los centros de datos (sites) del CEDETIC ningún material inflamable o peligroso (como por ejemplo cartón, cajas, papel o cualquier otro material similar).

- Los centros de datos (sites) del CEDETIC deben mantenerse limpios y ordenados en todo momento. Se deberá coordinar con el área correspondiente para establecer fecha y hora para realizar dicha actividad y serán supervisadas en todo momento por el Administrador de Bases de datos o el Administrador de Servidores.

- El Administrador de Bases de datos y/o el Administrador de Servidores deberán asegurarse de que al final de cualquier trabajo, todos los cables estén bien instalados y ordenados, dentro de sus gabinetes, y todas las puertas estén cerradas.

- No se debe arrastrar equipo sobre el piso falso de los centros de datos del CEDETIC, utilizar carretillas con llantas de caucho o carretillas con llantas de hierro, a menos que previamente se proteja el piso falso con cartón o cualquier otro material protector.

- No se permite el uso de aspiradoras, taladros o similares en el área de los equipos de servidores y telecomunicaciones, salvo que sea extremadamente necesario y autorizado por la dirección de CEDETIC.

- No está permitido levantar las baldosas del piso falso. Esta labor deberá ser solicitada a la dirección de CEDETIC, y deberá ser supervisada en todo momento por el Administrador de Bases de datos y/o el Administrador de Servidores.

- No se permiten las conexiones en cadena de varios PDU (regletas). Esto aumenta el riesgo de producción de incendios y una potencial sobrecarga de los circuitos eléctricos, resultando en la pérdida de energía del PDU o del circuito completo. La energía no debe exceder el 80% del total de la energía disponible por circuito.

2.3 Políticas de acceso a servidores

- Existe un grupo limitado de usuarios con acceso a los entornos de servidor, los perfiles por defecto son los siguientes:

  - Director del CEDETIC
  - Administrador de Servidores y Administrador de Bases de datos DBA
  - Jefes de departamentos del CEDETIC
  - Personal autorizado por la dirección del CEDETIC

- Las cuentas de acceso serán registradas de acuerdo al procedimiento especificado en el Manual de Procedimientos de la Dirección del CEDETIC.

- El acceso a los servidores es estrictamente de trabajo.

- No se permite utilizar servidores para almacenar información personal y/o ajena al Poder Judicial del Estado de Michoacán.

- Los roles de cada usuario estarán acorde a sus funciones y serán autorizados por el director del CEDETIC.

2.4 Políticas de acceso a bases de datos

1. El acceso a las bases de datos estará limitado solo al personal autorizado por la dirección del CEDETIC y/o el Jefe de departamento de Desarrollo de Software según los siguientes perfiles:

   - Director del CEDETIC
   - Administrador de Servidores y Administrador de Bases de datos (DBA)
   - Jefe del Departamento de Desarrollo de Software del CEDETIC
   - Personal del Departamento de Desarrollo de Software

2. Las cuentas de acceso serán registradas de acuerdo al procedimiento fijado en el Manual de Procedimientos de la Dirección del CEDETIC.

3. La cuenta de acceso es única y personal.

4. No se permite utilizar el acceso a las bases de datos con fines personales y/o que puedan poner en riesgo la seguridad de dicha información.

5. Cada usuario será asignado con perfiles y/o roles que así determine el Jefe del Departamento de Desarrollo de Software.

6. Ningún usuario podrá tener roles afines a dbadmin (SA) ya que éste pondría en riesgo la disponibilidad y la seguridad de los servicios de información.

7. Ningún usuario podrá realizar actividades del administrador de bases datos tales como:

   - Respaldos de bases de datos.
   - Recuperación de bases de datos.
   - Migración de servidores de bases de datos.
   - Creación, modificación y borrado de bases de datos.
   - Todas las funciones del Administrador de Bases de Datos que no están listadas en este inciso.

8. Derivado del punto anterior, cualquier requerimiento deberá ser coordinado entre el Jefe del Departamento de Desarrollo de Software y el Administrador de Bases de Datos o el Administrador de Servidores, o de así requerirse, del director del CEDETIC.

9. Los requerimientos del punto anterior, por tratarse de áreas internas del CEDETIC podrán ser atendidos verbalmente en reuniones internas registrándose en minutas de reunión, y/o vía correo electrónico.

10. Cualquier acceso para personal ajeno al departamento de Desarrollo de Software, a la administración de servidores y bases de datos y/o a la dirección del CEDETIC, deberá solicitarse por escrito a la dirección del CEDETIC.

2.5 Políticas de seguridad en bases de datos

1. Se debe mantener un esquema eficiente de respaldo de las bases de datos de los diferentes sistemas del Poder Judicial del Estado de Michoacán.

2. Se deberá contar con un control de respaldos que indique claramente frecuencia de respaldos de las bases de datos.

3. Se deberá automatizar el proceso de respaldos de las bases de datos a fin de optimizar el mismo.

4. Se deberá contar con un control que permita verificar que dichos respaldos se están generando de manera adecuada.

5. Se deberán realizar pruebas de restauración a partir de los respaldos generados, a fin de garantizar que los respaldos realizados están correctamente generados.

6. Se deberá tener claramente identificado el destino de los archivos de respaldos y el lugar donde serán reestablecidos a fin de garantizar un esquema de redundancia de bases de datos para el caso de fallas.

7. Se deberá tener al menos por duplicado los archivos de respaldos tanto en disco local como en unidades externas de almacenamiento a fin de garantizar la recuperación en caso de falla.

8. Con el fin de garantizar que la pérdida de información sea mínima en caso de falla general se determinará un plan de respaldo completo diario de preferencia durante la noche y generar respaldos de log de transacciones al menos cada hora durante la jornada laboral que comprende entre las 08:00 hrs y las 23:00 hrs. de lunes a sábado.

9. Además de almacenar los respaldos generados tanto en el servidor origen, y unidades de almacenamiento externo, se debe mantener copia de los mismos en dispositivos de almacenamiento en una ubicación diferente a la de los servidores, que deberá contar con las medidas de seguridad adecuadas.

2.6 Políticas de seguridad en archivos de datos (información general y anexos)

1. Se debe mantener un esquema eficiente de respaldo de archivos sensibles de las áreas que por su función la deben almacenar en servidores.

2. Se deberá contar con un control de respaldos que indique claramente la frecuencia de respaldos de los archivos.

3. Se deberá contar con un control que permita verificar que dichos respaldos se están generando de manera adecuada.

4. Se deberá tener claramente identificado el destino de los archivos de respaldos a fin de garantizar un esquema de redundancia de dichos archivos.

5. La información sensible como lo son los anexos de los sistemas de información jurisdiccionales, se deberá tener por duplicado, tanto en disco en servidores redundantes, como en unidades externas de almacenamiento a fin de garantizar la recuperación en caso de falla.

6. Además de almacenar los archivos sensibles tanto en el servidor origen, y unidades de almacenamiento externo, se debe mantener copia de los mismos en dispositivos de almacenamiento en una ubicación diferente a la de los servidores, que deberá contar con las medidas de seguridad adecuadas.

2.7 Políticas de seguridad y manejo de claves de acceso a sistemas operativos, equipos de red y sistemas manejadores de bases de datos

1. Las claves tanto de administrador de servidor como súper usuario "SA" de los sistemas manejadores de bases de datos se consideran confidenciales y de alta seguridad ya que sin ellas será imposible gestionar la plataforma base de operación.

2. Las contraseñas serán generadas tomando en cuenta las normas vigentes, caracterizándose por ser robustas y que no tengan relación obvia con el usuario, puesto de trabajo y el área o grupo de trabajo. Estas claves serán del conocimiento sólo del director del CEDETIC y del Administrador de servidores y/o del Administrador de Bases de Datos.

3. Las claves serán impresas y quedarán a resguardo dentro de sobre sellado y en la dirección de CEDETIC en lugar seguro y bajo llave.

4. Las claves por seguridad deberán ser modificadas de acuerdo a los siguientes casos:

   - Cambio de personal directivo del CEDETIC
   - Cambio de personal o responsabilidad del Administrador de Servidores y del Administrador de Bases de Datos del CEDETIC.
   - Periódicamente a consideración de la dirección del CEDETIC.
   - Por modificación o re implementación de los sistemas operativos y manejadores de bases de datos.

5. Otras claves y usuarios de acceso sensibles deberán permanecer en archivo electrónico considerado confidencial con clave de acceso seguro cuyo resguardo

estará a cargo del Administrador de bases de datos y/o del Administrador de servidores y el director del CEDETIC tendrá copia del mismo.

6. Las configuraciones de los equipos de red, serán resguardadas por el Departamento de Redes y Comunicaciones, en una unidad asignada en un servidor para tal efecto, teniendo solo acceso a estas, el Jefe del Departamento así como el Director del CEDETIC.

2.8 Políticas para la videograbación de una audiencia oral

- Las copias solo podrán ser solicitadas o autorizadas por el titular del órgano jurisdiccional al cual pertenece la grabación.

- Solo personal autorizado tendrá acceso al servidor donde se encuentran respaldados los videos de las audiencias.

- Los videos de las audiencias serán archivadas en el servidor con la nomenclatura asignada.

- Para las video grabaciones se debe seguir el Reglamento para el Manejo del Sistema y Archivo Digital de las Videograbaciones Generadas por Audiencias Orales en el Poder Judicial del Estado de Michoacán de Ocampo autorizado por el Consejo y las indicaciones giradas por el Consejo a los Juzgados Civiles y Familiares del Estado en el oficio SE/3416/2018 del 16 de julio de 2018.

2.9 Políticas para el desarrollo de sistemas de información

1. Toda elaboración de sistemas de información deberá estar orientada a satisfacer las necesidades de manejo de información de las áreas del Poder Judicial.

2. El diseño de los sistemas de información debe permitir, si se requiere, integrarse con otros sistemas.

3. Todos los sistemas de información desarrollados por el departamento de Desarrollo de software son propiedad del Poder Judicial.

4. El área solicitante deberá participar estrechamente con el departamento de Desarrollo de software durante el análisis, desarrollo e implementación de cualquier sistema de información.

5. Al terminar el desarrollo de un sistema de información, debe generarse la documentación necesaria para su entendimiento, lo cual al menos debe incluir el manual de usuario y el técnico.

6. De existir manuales de procedimientos vigentes para el área solicitante, el ingeniero de software asignado al proyecto de desarrollo del sistema de información debe tener conocimiento del contenido de ellos, a fin de reflejarlos en el sistema si se requiere.

7. Antes de liberar un nuevo sistema de información, éste debe ser sometido a pruebas de aceptación utilizando datos reales. En caso de nuevas versiones, será necesario realizar corridas en paralelo para verificar su correcto funcionamiento con respecto a la versión anterior.

8. Los archivos fuente de los sistemas de información deberán ser respaldados y controlados en sus versiones.

9. Las bases de datos de los sistemas de información serán respaldadas periódicamente de acuerdo a la frecuencia en sus transacciones y su importancia.

10. No se almacenarán las contraseñas sin encriptación en las bases de datos de los sistemas de información.

11. Las cuentas de usuario o contraseñas para el uso de un sistema de información deben ser desactivadas automáticamente después de que una persona deje de laborar en el área usuaria si utilizan las credenciales de la Intranet, o una vez que sea notificada su baja por el titular del área.

Importante: La dirección de CEDETIC es la responsable de proponer estas políticas y sus futuras modificaciones para que sean consideradas y aprobadas por el Consejo del Poder Judicial.

CEDETIC