

PODER JUDICIAL DEL ESTADO DE SINALOA



PLAN DE ACCIONES INSTITUCIONALES 2012

MANUAL DE POLÍTICAS Y ESTÁNDARES DE SEGURIDAD INFORMÁTICA PARA USUARIOS



DIRECCIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN Y
COMUNICACIONES

www.stj-sin.gob.mx

CONTENIDO

Propósito.....	1
Introducción.....	1
Objetivo.....	1
Alcance	2
Justificación.....	2
Sanciones por incumplimiento	2
Beneficios.....	2

1.-POLÍTICAS Y ESTÁNDARES DE SEGURIDAD DEL PERSONAL

Política	2
1.1. Obligaciones de los usuarios	2
1.2. Acuerdos de uso y confidencialidad	2
1.3. Entrenamiento en seguridad informática.....	3
1.4. Medidas disciplinarias.....	3

2.-POLÍTICAS Y ESTÁNDARES DE SEGURIDAD FÍSICA Y AMBIENTAL

Política	3
2.1. Resguardo y protección de la información.....	3
2.2. Controles de acceso físico.....	4
2.3. Seguridad en áreas de trabajo	4
2.4. Protección y ubicación de los equipos.....	4
2.5. Mantenimiento de equipo	5

2.6. Pérdida o transferencia de equipo.....	6
2.7. Uso de dispositivos especiales.....	6
2.8. Daño del equipo.....	7

3.-POLÍTICAS Y ESTÁNDARES DE SEGURIDAD Y ADMINISTRACIÓN DE OPERACIONES DE CÓMPUTO

Política.....	7
3.1. Uso de medios de almacenamiento.....	7
3.2. Instalación de Software.....	8
3.3. Identificación del incidente.....	9
3.4. Administración de la configuración.....	9
3.5. Seguridad de la red.....	9
3.6. Uso del correo electrónico.....	10
3.7. Controles contra código malicioso.....	11
3.8. Permisos de uso de Internet.....	12

4.-POLÍTICAS Y ESTÁNDARES DE CONTROLES DE ACCESO LÓGICO

Política.....	14
4.1. Controles de acceso lógico.....	14
4.2. Administración de privilegios.....	15
4.3. Equipo desatendido.....	16
4.4. Administración y uso de contraseñas.....	16
4.5. Control de accesos remotos.....	17

5.-POLÍTICAS Y ESTÁNDARES DE CUMPLIMIENTO DE SEGURIDAD INFORMÁTICA

Política	17
5.1. Derechos de propiedad intelectual.....	18
5.2. Revisiones del cumplimiento	18
5.3. Violaciones de Seguridad Informática.....	18
GLOSARIO DE TÉRMINOS	19

Propósito El presente documento tiene como finalidad dar a conocer las políticas y estándares de Seguridad Informática que deberán observar los usuarios de servicios de tecnologías de información, para proteger adecuadamente los activos tecnológicos y la información del Poder Judicial del Estado de Sinaloa.

Introducción La base para que cualquier organización pueda operar de una forma confiable en materia de Seguridad Informática comienza con la definición de políticas y estándares adecuados.

La Seguridad Informática es una función en la que se deben evaluar y administrar los riesgos, basándose en políticas y estándares que cubran las necesidades del Poder Judicial del Estado de Sinaloa en materia de seguridad.

Este documento se encuentra estructurado en cinco políticas generales de seguridad para usuarios de informática, con sus respectivos estándares que consideran los siguiente puntos:

- Seguridad de Personal
- Seguridad Física y Ambiental
- Administración de Operaciones de Cómputo
- Controles de Acceso Lógico
- Cumplimiento

Estas Políticas en seguridad informática se encuentran alineadas con el Estándar Británico ISO/IEC: 27002.

Objetivo Establecer y difundir las Políticas y Estándares de Seguridad Informática a todo el personal del Poder Judicial, para que sea de su conocimiento y cumplimiento en los recursos informáticos asignados.

Alcance	El documento define las Políticas y Estándares de Seguridad que deberán observar de manera obligatoria todos los usuarios para el buen uso del equipo de cómputo, aplicaciones y servicios informáticos del Poder Judicial del Estado de Sinaloa.
Justificación	La Dirección de Tecnologías de la Información y Comunicaciones del Supremo Tribunal de Justicia del Estado de Sinaloa está facultada para definir Políticas y Estándares en materia informática.
Sanciones por Incumplimiento	El incumplimiento al presente Manual podrá presumirse como causa de responsabilidad administrativa y/o penal, dependiendo de su naturaleza y gravedad, cuya sanción será aplicada por las autoridades competentes.
Beneficios	Las Políticas y Estándares de Seguridad Informática establecidos dentro de este documento son la base para la protección de los activos tecnológicos e información del Poder Judicial del Estado de Sinaloa.

1. POLÍTICAS Y ESTÁNDARES DE SEGURIDAD DEL PERSONAL

Política	Todo usuario de bienes y servicios informáticos se comprometen a conducirse bajo los principios de confidencialidad de la información y de uso adecuado de los recursos informáticos del Poder Judicial del Estado de Sinaloa, así como el estricto apego al Manual de Políticas y Estándares de Seguridad Informática para usuarios.
1.1.Obligaciones De los Usuarios	Es responsabilidad de los usuarios de bienes y servicios informáticos cumplir las Políticas y Estándares de Seguridad Informática para Usuarios del presente manual.
1.2 Acuerdos de uso y confidencialidad	Todos los usuarios de bienes y servicios informáticos del Supremo Tribunal de Justicia deberán conducirse conforme a los principios de confidencialidad y uso adecuado de los recursos informáticos y de información del Poder Judicial del Estado de Sinaloa, así como comprometerse a cumplir con lo establecido en el Manual de

Políticas y Estándares de Seguridad Informática para Usuarios.

- 1.3. Entrenamiento en Seguridad Informática
- Todo empleado del Supremo Tribunal de Justicia de nuevo ingreso deberá:
- Leer el Manual de Políticas y Estándares de Seguridad Informática para Usuarios del Poder Judicial del Estado de Sinaloa, el cual se encuentra disponible en el portal de internet del Supremo Tribunal de Justicia del Estado de Sinaloa, donde se dan a conocer las obligaciones para los usuarios y las sanciones que pueden aplicar en caso de incumplimiento.
- 1.4. Medidas disciplinarias
- 1.4.1. Cuando la Dirección identifique el incumplimiento al presente Manual remitirá el reporte o denuncia correspondiente al Órgano Interno de Control del Supremo Tribunal de Justicia, para los efectos de su competencia y atribuciones.

2.-POLÍTICAS Y ESTÁNDARES DE SEGURIDAD FÍSICA Y AMBIENTAL

- Política
- Los mecanismos de control y acceso físico para el personal y terceros deben permitir el acceso a las instalaciones y áreas restringidas del Poder Judicial del Estado de Sinaloa, sólo a personas autorizadas para la salvaguarda de los equipos de cómputo y de comunicaciones, así como las instalaciones y los diferentes Centros de Cómputo del Poder Judicial.
- 2.1 Resguardo y protección de la información
- 2.1.1. El usuario deberá reportar de forma inmediata a la Oficialía Mayor, cuando detecte que existan riesgos reales o potenciales para equipos de cómputo o comunicaciones, como pueden ser fugas de agua, conatos de incendio u otros.
- 2.1.2. El usuario tiene la obligación de proteger los CD-ROM, DVDs, memorias USB, tarjetas de memoria, discos externos, computadoras y dispositivos portátiles que se encuentren bajo su administración, aun cuando no se utilicen y contengan información reservada o confidencial.
- 2.1.3. Es responsabilidad del usuario evitar en todo momento la

fuga de la información del Poder Judicial que se encuentre almacenada en los equipos de cómputo personal que tenga asignados.

2.2. Controles de acceso físico

2.2.1. Cualquier persona que tenga acceso a las instalaciones del Poder Judicial del Estado de Sinaloa, deberá registrar en el Sistema de Ingreso (cuando ya se encuentre instalado), el equipo de cómputo, equipo de comunicaciones, medios de almacenamiento y herramientas que no sean propiedad del Poder Judicial del Estado de Sinaloa, el cual podrán retirar el mismo día, sin necesidad de trámite alguno.

En caso de que el equipo que no es propiedad del Poder Judicial del Estado de Sinaloa, permanezca dentro de la institución más de un día hábil, es necesario que el responsable del órgano del Poder Judicial en el que trabaja el dueño del equipo, elabore y firme oficio de autorización de salida.

2.3. Seguridad en áreas de trabajo

Los Centros de Cómputo del Poder Judicial del Estado son áreas restringidas, por lo que sólo el personal autorizado por la Dirección puede acceder a ellos.

2.4. Protección y ubicación de los equipos

2.4.1. Los usuarios no deben mover o reubicar los equipos de cómputo o de telecomunicaciones, instalar o desinstalar dispositivos, ni retirar sellos de los mismos sin la autorización de la Dirección, debiéndose solicitar a la misma en caso de requerir este servicio.

2.4.2. El área de soporte técnico de la Dirección será la encargada de generar el resguardo y recabar la firma del usuario informático como responsable de los activos informáticos que se le asignen y de conservarlos en la ubicación autorizada por la Dirección.

2.4.3. El equipo de cómputo asignado, deberá ser para uso exclusivo de las funciones asignadas al usuario del Poder Judicial del Estado de Sinaloa.

2.4.4. Será responsabilidad del usuario solicitar la capacitación necesaria para el manejo de las herramientas informáticas que se utilizan en su equipo, a fin de evitar riesgos por mal uso y para aprovechar al máximo las mismas.

2.4.5. Es responsabilidad de los usuarios almacenar su información únicamente en el directorio de trabajo que se le asigne, ya que los otros están destinados para archivos de programas y sistema operativo.

2.4.6. Mientras se opera el equipo de cómputo, no se deberán consumir alimentos o ingerir líquidos, a menos que sea en botellas de plástico.

2.4.7. Se debe evitar colocar objetos encima del equipo o cubrir los orificios de ventilación del monitor o del gabinete.

2.4.8. Se debe mantener el equipo informático en un entorno limpio y sin humedad.

2.4.9. El usuario debe asegurarse que los cables de conexión no sean pisados o aplastados al colocar otros objetos encima o contra ellos.

2.4.10. Cuando se requiera realizar cambios múltiples del equipo de cómputo derivado de reubicación de lugares físicos de trabajo, éstos deberán ser notificados con una semana de anticipación a la Dirección a través de un plan detallado de movimientos debidamente autorizados por el titular del área que corresponda.

2.4.11. Queda prohibido que el usuario abra o desarme los equipos de cómputo, porque con ello perdería la garantía que proporciona el proveedor de dicho equipo.

2.5. Mantenimiento de equipo

2.5.1. Únicamente el personal autorizado de la Dirección podrá llevar a cabo los servicios y reparaciones al equipo informático, por lo que los usuarios deberán solicitar la identificación del personal designado antes de permitir el acceso a sus equipos.

2.5.2. Los usuarios deberán asegurarse de respaldar la información que considere relevante cuando el equipo sea enviado a reparación y borrar aquella información sensible que se encuentre en el equipo previendo así la pérdida involuntaria de información, derivada de proceso de reparación, solicitando la asesoría del personal de la Dirección.

2.6. Pérdida o transferencia de equipo

2.6.1. El usuario que tenga bajo su resguardo algún equipo de cómputo será responsable de su uso y custodia; en consecuencia, responderá por dicho bien de acuerdo a la normatividad vigente en los casos de robo, extravío o pérdida del mismo.

2.6.2. El resguardo para las laptops, tiene el carácter de personal y será intransferible. Por tal motivo, queda prohibido su préstamo.

2.6.3. El usuario deberá dar aviso de inmediato a la Dirección de la desaparición, robo o extravío del equipo de cómputo o accesorios bajo su resguardo.

2.7. Uso de dispositivos especiales

2.7.1. El uso de los grabadores de discos compactos es exclusivo para respaldos de información que por su volumen así lo justifiquen.

2.7.2. La asignación de este tipo de equipo será previa justificación por escrito y autorización del titular o jefe inmediato correspondiente.

2.7.3. El usuario que tenga bajo su resguardo este tipo de dispositivos será responsable del buen uso que se le dé.

2.7.4. Los módems internos deberán existir solo en las computadoras portátiles y no se deberán utilizar dentro de las instalaciones de la institución para conectarse a ningún servicio de información externo, excepto cuando lo autorice la Dirección.

2.8. Daño del equipo El equipo de cómputo o cualquier recurso de tecnología de información que sufra alguna descompostura por maltrato, descuido o negligencia por parte del usuario, deberá cubrir el valor de la reparación o reposición del equipo o accesorio afectado. Para tal caso la determinará la causa de dicha descompostura.

3. POLÍTICAS, ESTÁNDARES DE SEGURIDAD Y ADMINISTRACIÓN DE OPERACIONES DE CÓMPUTO

Política Los usuarios deberán utilizar los mecanismos institucionales para proteger la información que reside y utiliza la infraestructura del Poder Judicial del Estado de Sinaloa. De igual forma, deberán proteger la información reservada o confidencial que por necesidades institucionales deba ser almacenada o transmitida, ya sea dentro de la red interna del Poder Judicial del Estado de Sinaloa o hacia redes externas como internet.

Los usuarios del Poder Judicial del Estado de Sinaloa que hagan uso de equipo de cómputo, deben conocer y aplicar las medidas para la prevención de código malicioso como pueden ser virus, *malware* o *spyware*. El usuario puede acudir a la Dirección , o al representante de ésta en su zona, para solicitar asesoría.

3.1. Uso de medios de almacenamiento 3.1.1. Toda solicitud para utilizar un medio de almacenamiento de información compartido, deberá contar con la autorización del Juez o jefe inmediato del usuario y del titular del área dueña de la información.

Dicha solicitud deberá explicar en forma clara y concisa los fines para los que se otorgará la autorización, ese documento se presentará con sello y firma del titular de área o Juez a la Dirección o al representante de ésta en su zona..

3.1.2. Los usuarios deberán respaldar de manera periódica la información sensible y crítica que se encuentre en sus computadoras personales o estaciones de trabajo, solicitando asesoría de la Dirección o al representante de ésta en su zona,

para que dichos asesores determinen el medio en que se realizará dicho respaldo.

3.1.3. En caso de que por el volumen de información se requiera algún respaldo en CD, este servicio deberá solicitarse por escrito al Titular de la Dirección, y deberá contar con la firma del titular del área de adscripción del solicitante.

3.1.4. Los trabajadores del Poder Judicial del Estado de Sinaloa deben conservar los registros o información que se encuentra activa y aquella que ha sido clasificada como reservada o confidencial, de conformidad a las disposiciones que emita la Unidad de Acceso a la Información Pública del Poder Judicial del Estado de Sinaloa, en términos de Ley de Acceso a la Información pública del Estado de Sinaloa, Acuerdo General que establece el órgano, y demás criterios y procedimientos establecidos en esta materia.

3.1.5. Las actividades que realicen los usuarios del Poder Judicial del Estado de Sinaloa en la infraestructura de Tecnología de la Información son registradas y susceptibles de auditoría.

3.2. Instalación de Software

3.2.1. Los usuarios que requieran la instalación de software que no sea propiedad del Poder Judicial del Estado de Sinaloa, deberán justificar su uso y solicitar su autorización a la Dirección, a través de un oficio firmado por el titular del área de su adscripción, indicando el equipo de cómputo donde se instalará el software y el período que permanecerá dicha instalación, siempre y cuando el dueño del software presente la factura de compra de dicho software.

Si el dueño del software no presenta la factura de compra del software, el personal asignado por la Dirección procederá de manera inmediata a desinstalar dicho software.

3.2.2. Se considera una falta grave el que los usuarios instalen cualquier tipo de programa (*software*) en sus computadoras,

estaciones de trabajo, servidores, o cualquier equipo conectado a la red del Poder Judicial del Estado de Sinaloa, que no esté autorizado por la Dirección.

3.3. Identificación del incidente 3.3.1. El usuario que sospeche o tenga conocimiento de la ocurrencia de un incidente de seguridad informática deberá reportarlo a la Dirección o al representante de ésta en su zona, lo antes posible, indicando claramente los datos por los cuales lo considera un incidente de seguridad informática.

3.3.2. Cuando exista la sospecha o el conocimiento de que información confidencial o reservada ha sido revelada, modificada, alterada o borrada sin la autorización de las unidades administrativas competentes, el usuario informático deberá notificar al titular de su adscripción.

3.3.3. Cualquier incidente generado durante la utilización u operación de los activos de tecnología de información del Poder Judicial del Estado de Sinaloa, debe ser reportado a la Dirección.

3.4. Administración de la configuración Los usuarios de las áreas del Poder Judicial del Estado de Sinaloa no deben establecer redes de área local, conexiones remotas a redes internas o externas, intercambio de información con otros equipos de cómputo utilizando el protocolo de transferencia de archivos (FTP), u otro tipo de protocolo para la transferencia de información empleando la infraestructura de red del Poder Judicial del Estado de Sinaloa, sin la autorización por escrito de la Dirección.

3.5. Seguridad de la red Será considerado como un ataque a la seguridad informática y una falta grave, cualquier actividad no autorizada por la Dirección en la cual los usuarios realicen la exploración de los recursos informáticos en la red del Poder Judicial del Estado de Sinaloa, así como de las aplicaciones que sobre dicha red operan, con fines de detectar y mostrar una posible vulnerabilidad.

3.6. Uso del correo electrónico

3.6.1. Los usuarios no deben usar cuentas de correo electrónico asignadas a otras personas, ni recibir mensajes en cuentas de otros. Si fuera necesario leer el correo de alguien más (mientras esta persona se encuentra fuera o ausente), el usuario ausente debe redireccionar el correo a otra cuenta de correo interno, quedando prohibido hacerlo a una dirección de correo electrónico externa al Poder Judicial del Estado de Sinaloa, a menos que cuente con la autorización del titular del área de adscripción.

3.6.2. Los usuarios deben tratar los mensajes de correo electrónico y archivos adjuntos como información que es propiedad del Poder Judicial del Estado de Sinaloa (si es propiedad del Poder Judicial del Estado es información pública). Los mensajes de correo electrónico deben ser manejados como una comunicación privada y directa entre emisor y receptor.

3.6.3. Los usuarios podrán enviar información reservada y/o confidencial exclusivamente a personas autorizadas y en el ejercicio estricto de sus funciones y atribuciones, a través del correo institucional que le proporcionó la Dirección.

3.6.4. El Poder Judicial del Estado de Sinaloa, se reserva el derecho de acceder y revelar todos los mensajes enviados por este medio para cualquier propósito y revisar las comunicaciones vía correo electrónico de personal que ha comprometido la seguridad violando políticas de Seguridad Informática del Poder Judicial del Estado de Sinaloa o realizado acciones no autorizadas.

Como la información del correo electrónico institucional del Poder Judicial del Estado de Sinaloa es privada, la única forma en la que puede ser revelada es mediante una orden judicial.

3.6.5. El usuario debe de utilizar el correo electrónico del Poder Judicial del Estado de Sinaloa, única y exclusivamente para los recursos que tenga asignados y las facultades que les hayan sido atribuidas para el desempeño de su empleo, cargo o comisión, quedando prohibido cualquier otro uso distinto.

3.6.6. La asignación de una cuenta de correo electrónico externo, deberá solicitarse por escrito a la Dirección o al representante de ésta en su zona, señalando los motivos por los que se desea el servicio. Esta solicitud deberá contar con el visto bueno del titular del área que corresponda.

3.6.7. Queda prohibido falsear, esconder, suprimir o sustituir la identidad de un usuario de correo electrónico.

3.7. Controles contra código malicioso

3.7.1. Para prevenir infecciones por virus informáticos, los usuarios del Poder Judicial del Estado de Sinaloa, deben evitar hacer uso de cualquier clase de software que no haya sido proporcionado y validado por la Dirección.

3.7.2. Los usuarios del Poder Judicial del Estado de Sinaloa, deben verificar que la información y los medios de almacenamiento, considerando al menos memorias USB, discos flexibles, CD's, estén libres de cualquier tipo de código malicioso, para lo cual deben ejecutar el software antivirus autorizado por la Dirección.

3.7.3. El usuario debe verificar mediante el software de antivirus autorizado por la Dirección que estén libres de virus todos los archivos de computadora, bases de datos, documentos u hojas de cálculo, etc. que sean proporcionados por personal externo o interno, considerando que tengan que ser descomprimidos.

3.7.4. Ningún usuario del Poder Judicial del Estado de Sinaloa debe intencionalmente escribir, generar, compilar, copiar, propagar, ejecutar o tratar de introducir código de computadora diseñado para autoreplicarse, dañar o en otros casos impedir el funcionamiento de cualquier memoria de computadora, archivos de sistema o software. Tampoco debe probarlos en cualquiera de los ambientes o plataformas del Poder Judicial del Estado de Sinaloa. El incumplimiento de este estándar será considerado una falta grave.

3.7.5. Ningún usuario ni empleado del Poder Judicial del Estado de Sinaloa o personal externo podrá bajar o descargar software de sistemas, boletines electrónicos, sistemas de correo electrónico, de mensajería instantánea y redes de comunicaciones externas, sin la debida autorización de la Dirección de Tecnologías de Información y Comunicaciones del Supremo Tribunal de Justicia.

3.7.6. Cualquier usuario que sospeche de alguna infección por virus de computadora, deberá dejar de usar inmediatamente el equipo y llamar a la Dirección para la detección y erradicación del virus.

3.7.7. Cada usuario que tenga bajo su resguardo algún equipo de cómputo personal portátil, será responsable de solicitar de manera periódica a la Dirección las actualizaciones del software de antivirus.

3.7.8. Los usuarios no deberán alterar o eliminar las configuraciones de seguridad para detectar y/o prevenir la propagación de virus que sean implantadas por la Dirección en programas tales como:

- Antivirus;
- Correo electrónico;
- Paquetería Office;
- Navegadores; u
- Otros programas.

3.7.9. Debido a que algunos virus son extremadamente complejos, ningún usuario del Poder Judicial del Estado de Sinaloa debe intentar erradicarlos de las computadoras, lo indicado es llamar al personal de la Dirección para que sean ellos quienes lo solucionen.

3.8. Permisos de uso de Internet

3.8.1. El acceso a internet provisto a los usuarios del Poder Judicial del Estado de Sinaloa es exclusivamente para las actividades relacionadas con las necesidades del puesto y función que desempeña. En caso de daño a la imagen de la institución se procederá de acuerdo a lo que determine el Órgano Interno de Control del Supremo Tribunal de Justicia del Estado de Sinaloa.

3.8.2. La asignación del servicio de internet, deberá solicitarse por escrito a la Dirección, señalando los motivos por los que se desea el servicio. Esta solicitud deberá contar con el visto bueno del titular del área correspondiente.

3.8.3. Todos los accesos a internet tienen que ser realizados a través de los canales de acceso provistos por el Poder Judicial del Estado de Sinaloa.

3.8.4. Los usuarios con acceso a Internet del Poder Judicial del Estado de Sinaloa tienen que reportar todos los incidentes de seguridad informática a la, inmediatamente después de su identificación, indicando claramente que se trata de un incidente de seguridad informática.

3.8.5. El acceso y uso de módem en el Supremo Tribunal de Justicia tiene que ser previamente autorizado por la Dirección.

3.8.7. Los usuarios con servicio de navegación en internet al utilizar el servicio aceptan que:

- Serán sujetos de monitoreo de las actividades que realizan en internet.
- Saben que existe la prohibición al acceso de páginas no autorizadas.
- Saben que existe la prohibición de transmisión de archivos reservados o confidenciales no autorizados.
- Saben que existe la prohibición de descarga de *software* sin la autorización de la Dirección.
- La utilización de internet es para el desempeño de su función y puesto en el Poder Judicial del Estado de Sinaloa y no para propósitos personales.

3.8.8. Los esquemas de permisos de acceso a internet y servicios de mensajería instantánea son:

NIVEL 1: Sin restricciones: Los usuarios podrán navegar en

las páginas que así deseen, así como realizar descargas de información multimedia en sus diferentes presentaciones y acceso total a servicios de mensajería instantánea.

NIVEL 2: Internet restringido y mensajería instantánea: Los usuarios podrán hacer uso de internet y servicios de mensajería instantánea, aplicándose las políticas de seguridad y navegación.

NIVEL 3: Internet restringido y sin mensajería instantánea: Los usuarios sólo podrán hacer uso de internet aplicándose las políticas de seguridad y navegación

NIVEL 4: El usuario no tendrá acceso a Internet ni a servicios de mensajería instantánea.

4.POLÍTICAS Y ESTÁNDARES DE CONTROLES DE ACCESO LÓGICO

Política Cada usuario es responsable del mecanismo de control de acceso que le sea proporcionado; esto es, de su identificador de usuario (*userID*) y contraseña (*password*) necesarios para acceder a la información y a la infraestructura tecnológica del Poder Judicial del Estado de Sinaloa, por lo cual deberá mantenerlo de forma confidencial.

La Presidencia del Supremo Tribunal de Justicia del Estado de Sinaloa, es el único que puede otorgar la autorización para que se tenga acceso a la información que se encuentra en la infraestructura tecnológica del Poder Judicial del Estado de Sinaloa, otorgándose los permisos mínimos necesarios para el desempeño de sus funciones, con apego al principio "Necesidad de saber".

4.1. Controles de acceso lógico 4.1.1. El acceso a la infraestructura tecnológica del Poder Judicial del Estado de Sinaloa para personal externo debe ser autorizado al menos por un titular de área del Poder Judicial del Estado de Sinaloa, quien deberá notificarlo por oficio a la Dirección, quien lo habilitará.

4.1.2. Está prohibido que los usuarios utilicen la infraestructura tecnológica del Poder Judicial del Estado para obtener acceso no autorizado a la información u otros sistemas de información del Poder Judicial del Estado de Sinaloa.

4.1.3. Todos los usuarios de servicios de información son responsables por su identificador de usuario y contraseña que recibe para el uso y acceso de los recursos.

4.1.4. Todos los usuarios deberán autenticarse por los mecanismos de control de acceso provistos por la Dirección antes de poder usar la infraestructura tecnológica del Poder Judicial del Estado de Sinaloa.

4.1.5. Los usuarios no deben proporcionar información a personal externo, de los mecanismos de control de acceso a las instalaciones e infraestructura tecnológica del Poder Judicial del Estado de Sinaloa, a menos que se tenga autorización de la Dirección.

4.1.6. Cada usuario que accede a la infraestructura tecnológica del Poder Judicial del Estado de Sinaloa debe contar con un identificador de usuario único y personalizado, por lo cual no está permitido el uso de un mismo identificador de usuario por varios usuarios.

4.1.7. Los usuarios tienen prohibido compartir su identificador de usuario y contraseña, ya que todo lo que ocurra con ese identificador y contraseña será responsabilidad exclusiva del usuario al que pertenezcan, salvo prueba de que le fueron usurpados esos controles.

4.1.8. Los usuarios tienen prohibido usar el identificador de usuario y contraseña de otros, aunque ellos les insistan en usarlo.

4.2.
Administración
de privilegios

4.2.1. Cualquier cambio en los roles y responsabilidades de los usuarios que modifique sus privilegios de acceso a la infraestructura tecnológica del Poder Judicial del Estado de Sinaloa,

deberán ser notificados por escrito o vía correo electrónico a la Dirección con el visto bueno del titular del área solicitante, para realizar el ajuste.

4.3. Equipo desatendido

Los usuarios deberán mantener sus equipos de cómputo con controles de acceso como contraseñas y protectores de pantalla (previamente instalados y autorizados por la Dirección, como una medida de seguridad cuando el usuario necesita ausentarse de su escritorio por un tiempo.

4.4. Administración y uso de contraseñas

4.4.1. La asignación de la contraseña para acceso a la red y la contraseña para acceso a sistemas, debe ser realizada de forma individual, por lo que queda prohibido el uso de contraseñas compartidas está prohibido.

4.4.2. Cuando un usuario olvide, bloquee o extravíe su contraseña, deberá reportarlo por escrito a la Dirección, indicando si es de acceso a la red o a módulos de sistemas desarrollados por la Dirección, para que se le proporcione una nueva contraseña.

4.4.3. La obtención o cambio de una contraseña debe hacerse de forma segura; el usuario deberá acreditarse ante la Dirección como empleado del Poder Judicial del Estado.

4.4.4. Está prohibido que los identificadores de usuarios y contraseñas se encuentren de forma visible en cualquier medio impreso o escrito en el área de trabajo del usuario, de manera de que se permita a personas no autorizadas su conocimiento.

4.4.5. Todos los usuarios deberán observar los siguientes lineamientos para la construcción de sus contraseñas:

- No deben contener números consecutivos;
- Deben estar compuestos de al menos seis (6) caracteres y máximo diez (10). Estos caracteres deben ser alfanuméricos, o sea, números y letras;

- Deben ser difíciles de adivinar, esto implica que las contraseñas no deben relacionarse con el trabajo o la vida personal del usuario; y
- Deben ser diferentes a las contraseñas que se hayan usado previamente.

4.4.7. La contraseña podrá ser cambiada por requerimiento del dueño de la cuenta.

4.4.8. Todo usuario que tenga la sospecha de que su contraseña es conocido por otra persona, tendrá la obligación de cambiarlo inmediatamente.

4.4.9. Los usuarios no deben almacenar las contraseñas en ningún programa o sistema que proporcione esta facilidad.

4.4.10. Los cambios o desbloqueo de contraseñas solicitados por el usuario a la Dirección serán solicitados mediante oficio sellado y firmado por el jefe inmediato del usuario que lo requiere.

4.5. Control de accesos remotos

4.5.1. Está prohibido el acceso a redes externas por vía de cualquier dispositivo, cualquier excepción deberá ser documentada y contar con el visto bueno de la Dirección.

4.5.2. La administración remota de equipos conectados a internet no está permitida, salvo que se cuente con la autorización y con un mecanismo de control de acceso seguro autorizado por la Dirección.

5. POLÍTICAS Y ESTÁNDARES DE CUMPLIMIENTO DE SEGURIDAD INFORMÁTICA

Política

De acuerdo al artículo 71 del Reglamento Interior del Supremo Tribunal de Justicia del Estado de Sinaloa: *"La Dirección de Tecnologías de la Información y Comunicaciones, es la encargada de fijar las bases de la política informática que permitan conocer y planear el desarrollo tecnológico al interior del Poder Judicial"*

5.1. Derechos de Propiedad Intelectual 5.1.1. Está prohibido por las leyes de derechos de autor y por el Poder Judicial del Estado de Sinaloa, realizar copia no autorizadas de *software*, ya sea adquirido o desarrollado por el Poder Judicial del Estado de Sinaloa.

5.1.2. Los sistemas desarrollados por personal, interno o externo, que sea parte de la Dirección, o sea coordinado por ésta, son propiedad intelectual del Poder Judicial del Estado de Sinaloa.

5.2. Revisiones del cumplimiento 5.2.1. La Dirección realizará acciones de verificación del cumplimiento del Manual de Políticas y Estándares de Seguridad Informática para usuarios.

5.2.2. La Dirección podrá implementar mecanismos de control que permitan identificar tendencias en el uso de recursos informáticos del personal interno o externo, para revisar la actividad de procesos que ejecuta y la estructura de los archivos que se procesan. El mal uso de los recursos informáticos que sea detectado será reportado conforme a lo indicado en la Política de Seguridad del Personal.

5.3. Violaciones de seguridad informática 5.3.1. Está prohibido el uso de herramientas de hardware o software para violar los controles de seguridad informática. A menos que se autorice por la Dirección.

5.3.2. Está prohibido realizar pruebas de controles de los diferentes elementos de Tecnología de la Información.

Ninguna persona puede probar o intentar comprometer los controles internos a menos de contar con la aprobación de la Dirección, con excepción de los Órganos Fiscalizadores.

5.3.3. Ningún usuario del Poder Judicial del Estado debe probar o intentar probar fallas de la Seguridad Informática identificadas o conocidas, a menos que estas pruebas sean controladas y aprobadas por la Dirección.

5.3.4. No se debe intencionalmente escribir, generar, compilar,

copiar, coleccionar, propagar, ejecutar, introducir cualquier tipo de código (programa) conocidos como virus, *malware*, *spyware*, o similares diseñado para autoreplicarse, dañar, afectar el desempeño, acceso a las computadoras, redes e información del Poder Judicial del Estado.

Para los efectos del presente manual, se escribe el presente glosario de términos:

GLOSARIO DE TÉRMINOS

TÉRMINO	SIGNIFICADO
(A)	
Acceso	Es el privilegio de una persona para utilizar un objeto o infraestructura.
Acceso Físico	Es la actividad de ingresar a un área.
Acceso Lógico	Es la habilidad de comunicarse y conectarse a un activo tecnológico para utilizarlo.
Acceso Remoto	Conexión de dos dispositivos de cómputo ubicados en diferentes lugares físicos por medio de líneas de comunicación, ya sean telefónicas o por medio de redes de área amplia, que permiten el acceso de aplicaciones e información de la red. Este tipo de acceso normalmente viene acompañado de un sistema robusto de autenticación.
Antivirus	Programa que busca y eventualmente elimina los virus informáticos que pueden haber infectado un disco rígido, o cualquier sistema de almacenamiento electrónico de información.
Ataque	Actividades encaminadas a quebrantar las protecciones establecidas de un activo específico, con la finalidad de obtener acceso a ese archivo y lograr afectarlo.
(B)	
Base de datos	Colección almacenada de datos relacionados, requeridos por las organizaciones e individuos para que cumplan con los requerimientos de proceso de información y recuperación de datos.
(C)	
Confidencialidad	Se refiere a la obligación de los servidores judiciales a no divulgar

	información a personal no autorizado para su conocimiento.
Contraseña	Secuencia de caracteres utilizados para determinar que un usuario específico requiere acceso a una computadora personal, sistema, aplicación o red en particular.
Control de Acceso	Es un mecanismo de seguridad diseñado para prevenir, salvaguardar y detectar acceso no autorizado y permitir acceso autorizado a un activo.
Copyright	Derecho que tiene un autor, incluido el autor de un programa informático sobre todas y cada una de sus obras y que le permite decidir en qué condiciones han de ser éstas reproducidas y distribuidas. Aunque este derecho es legalmente irrenunciable puede ser ejercido de forma tan restrictiva o tan generosa como el autor decida.
(D)	
Dirección	Se refiere a la Dirección de Tecnologías de la Información y Comunicaciones del Supremo Tribunal de Justicia del Estado de Sinaloa.
Disponibilidad	Se refiere a que la información esté disponible en el momento que se necesite.
(E)	
Estándar	Los estándares son actividades, acciones, reglas o regulaciones obligatorias diseñadas para proveer a las políticas de la estructura y dirección que requieren para ser efectivas y significativas.
(F)	
Falta administrativa	Acción u omisión contemplada por la normatividad aplicable a la actividad de un servidor judicial, mediante la cual se finca responsabilidad y se sanciona esa acción u omisión.
FTP	Protocolo de transferencia de archivos. Es un protocolo estándar de comunicación que proporciona un camino simple para extraer y colocar archivos compartidos entre computadoras sobre un ambiente de red.
(G)	
Gusano	Programa de computadora que puede replicarse a sí mismo y enviar copias de una computadora a otra a través de conexiones de la red, antes de su llegada al nuevo sistema, el gusano debe estar activado para replicarse y propagarse nuevamente, además de la

	propagación, el gusano desarrolla en los sistemas de cómputo funciones no deseadas.
(H)	
Hardware	Se refiere a las características técnicas y físicas de las computadoras.
Herramientas de seguridad	Son mecanismos de seguridad automatizados que sirven para proteger o salvaguardar a la infraestructura tecnológica de una Comisión.
(I)	
Identificador de Usuario	Nombre de usuario (también referido como UserID) único asignado a un servidor judicial para el acceso a equipos y sistemas desarrollados, permitiendo su identificación en los registros.
Impacto	Magnitud del daño ocasionado a un activo en caso de que se materialice.
Incidente de Seguridad	Cualquier evento que represente un riesgo para la adecuada conservación de confidencialidad, integridad o disponibilidad de la información utilizada en el desempeño de nuestra función.
Integridad	Se refiere a la pérdida ó deficiencia en la autorización, totalidad ó exactitud de la información de la organización. Es un principio de seguridad que asegura que la información y los sistemas de información no sean modificados de forma intencional.
Internet	Es un sistema a nivel mundial de computadoras conectadas a una misma red, conocida como la red de redes (world wide web) en donde cualquier usuario consulta información de otra computadora conectada a esta red e incluso sin tener permisos.
Intrusión	Es la acción de introducirse o acceder sin autorización a un activo.
(M)	
Maltrato	Son todas aquellas acciones que de manera voluntaria o involuntaria el usuario ejecuta y como consecuencia daña los recursos tecnológicos propiedad del Supremo Tribunal de Justicia. Se contemplan dentro de éste al descuido y la negligencia.
Malware	Código malicioso desarrollado para causar daños en equipos informáticos, sin el consentimiento del propietario. Dentro de estos códigos se encuentran: virus, <i>spyware</i> , <i>troyanos</i> , <i>rootkits</i> , <i>backdoors</i> , <i>adware</i> y gusanos.
Mecanismos de seguridad o de	Es un control manual o automático para proteger la información, activos tecnológicos, instalaciones, etc. que se utiliza para disminuir

control	la probabilidad de que una vulnerabilidad exista, sea explotada, o bien ayude a reducir el impacto en caso de que sea explotada.
Medios de almacenamiento magnéticos	Son todos aquellos medios en donde se pueden almacenar cualquier tipo de información (diskettes, CD's, DVD's, etc.)
Módem	Es un aparato electrónico que se adapta una terminal o computadora y se conecta a una red de. Los módems convierten los pulsos digitales de una computadora en frecuencias dentro de la gama de audio del sistema telefónico. Cuando actúa en calidad de receptor, un módem decodifica las frecuencias entrantes.
(N)	
"Necesidad de saber" principio	Es un principio o base de seguridad que declara que los usuarios deben tener exclusivamente acceso a la información, instalaciones o recursos tecnológicos de información entre otros que necesitan para realizar o completar su trabajo cumpliendo con sus roles y responsabilidades dentro de la Comisión.
Normatividad	Conjunto de lineamientos que deberán seguirse de manera obligatoria para cumplir un fin dentro de una organización.
(P)	
Password	Véase Contraseña.
(R)	
Respaldo	Archivos, equipo, datos y procedimientos disponibles para el uso en caso de una falla o pérdida, si los originales se destruyen o quedan fuera de servicio.
Riesgo	Es el potencial de que una amenaza tome ventaja de una debilidad de seguridad (vulnerabilidad) asociadas con un activo, comprometiendo la seguridad de éste. Usualmente el riesgo se mide por el impacto que tiene.
(S)	
Servidor	Computadora que responde peticiones o comandos de una computadora cliente. El cliente y el servidor trabajan conjuntamente para llevar a cabo funciones de aplicaciones distribuidas. El servidor es el elemento que cumple con la colaboración en la arquitectura cliente-servidor.
Sitio Web	El sitio web es un lugar virtual en el ambiente de internet, el cual

	proporciona información diversa para el interés del público, donde los usuarios deben proporcionar la dirección de dicho lugar para llegar a él.
Software	Programas y documentación de respaldo que permite y facilita el uso de la computadora. El software controla la operación del hardware.
Spyware	Código malicioso desarrollado para infiltrar a la información de un equipo o sistema con la finalidad de extraer información sin la autorización del propietario.
(U)	
UserID	Véase Identificador de Usuario.
Usuario	Este término es utilizado para distinguir a cualquier persona que utiliza algún sistema, computadora personal o dispositivo (hardware).
(V)	
Virus	Programas o códigos maliciosos diseñados para esparcirse y copiarse de una computadora a otra por medio de los enlaces de telecomunicaciones o al compartir archivos o medios de almacenamiento magnético de computadoras.
Vulnerabilidad	Es una debilidad de seguridad o brecha de seguridad, la cual indica que el activo es susceptible a recibir un daño a través de un ataque, ya sea intencional o accidental.



PODER JUDICIAL