PODER JUDICIAL DEL ESTADO DE SINALOA

SUPREMO TRIBUNAL DE JUSTICIA

DIRECCIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIONES

MANUAL DE POLÍTICAS Y ESTÁNDARES DE SEGURIDAD INFORMÁTICA PARA USUARIO DEL PODER JUDICIAL DEL ESTADO DE SINALOA (VERSIÓN 2.2)

UNIDAD RESPONSABLE:

ADMINISTRACIÓN DE PROYECTOS Y ESTÁNDARES TECNOLÓGICOS

PODER JUDICIAL DEL ESTADO DE SINALOA

VERSIÓN 2.0 PLAN DE ACCIONES INSTITUCIONALES 2017

MANUAL DE POLÍTICAS Y ESTÁNDARES DE SEGURIDAD INFORMÁTICA PARA USUARIOS

DIRECCIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIONES

www.stj-sin.gob.mx

Contenido

1. OBJETIVOS GENERALES

Establecer y difundir las Políticas y Estándares de Seguridad Informática que deberán observar los usuarios de servicios de Tecnologías de la Información para proteger adecuadamente los activos tecnológicos y la información del Poder Judicial del Estado de Sinaloa.

2. OBJETIVOS ESPECÍFICOS

- Operar de una forma confiable en materia de Seguridad Informática a través de la definición de Políticas y Estándares Adecuados.
- Evaluar y administrar los riesgos de la Seguridad Informática en base a Políticas y Estándares que cubran las necesidades del Poder Judicial del Estado de Sinaloa.
- Estructurar en 5 (CINCO) Políticas Generales de Seguridad para Usuarios de informática y cubrir:
  - Seguridad de Personal
  - Seguridad Física y Ambiental
  - Administración de Operaciones de Cómputo
  - Controles de Acceso Lógico
  - Cumplimiento de Seguridad Informática
- Alinear las Políticas en Seguridad Informática según lo establece el Estándar Británico en sus mejores prácticas de ISO/IEC: 27002:2013 así como la norma ISO 27001:2013.

3. GLOSARIO

I. DTIC: Dirección de Tecnologías de la Información y Comunicaciones.

4. MARCO LEGAL

El Reglamento Interior del Supremo Tribunal de Justicia del Estado de Sinaloa establece, en su artículo 71, que compete a la DTIC fijar las bases de la política informática, para planear el desarrollo tecnológico del Poder Judicial.

5. ALCANCE

El documento define las Políticas y los 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.

6. JUSTIFICACIÓN

DTIC está facultada para definir Políticas y Estándares en materia informática.

7. 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.

8. OBLIGACIÓN PARA TITULARES DE ÁREAS JURISDICCIONALES Y/O ADMINISTRATIVAS

Cada Titular de Área tendrá la responsabilidad de informar a los empleados de nuevo ingreso, que es obligatorio entrar a www.stj-sin.gob.mx, para que lean el Manual de Políticas y Estándares de Seguridad Informática y con ello conozcan las responsabilidades informáticas que implican ser nuevo empleado del Poder Judicial del Estado de Sinaloa.

9. MEDIDAS DISCIPLINARIAS

Cuando DTIC 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.

10. PRIMERA POLÍTICA GENERAL: POLÍTICAS Y ESTÁNDARES DE SEGURIDAD PERSONAL

POLÍTICA:

Todo usuario de bienes y servicios informáticos se compromete 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.

10.1. Obligaciones de los Usuarios

Es responsabilidad de los usuarios de bienes y servicios informáticos del Poder Judicial del Estado de Sinaloa, cumplir las Políticas y Estándares de Seguridad Informática para Usuarios del presente manual.

10.2 Acuerdos de uso y confidencialidad

Todos los usuarios de bienes y servicios informáticos del Poder Judicial del Estado de Sinaloa 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.

11. SEGUNDA POLÍTICA GENERAL: "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 área 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.

11.1. Resguardo y protección de la información

11.1.1. El usuario deberá reportar de forma inmediata a Administración de Infraestructura Física, Servicios y Suministros de 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.

11.1.2. 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 resguardo, aún cuando no se utilicen y contengan información reservada o confidencial.

11.1.3. Es responsabilidad del usuario evitar en todo momento la fuga de la información del Poder Judicial del Estado de Sinaloa que se encuentre almacenada en los equipos de cómputo personal que tenga asignados.

11.2. Seguridad en áreas de trabajo

Los Centros de Datos de DTIC ubicados en Zona Norte, Centro y Sur del Poder Judicial del Estado de Sinaloa son áreas restringidas, por lo que sólo el personal autorizado por DTIC o sus representantes en la zona puede acceder a ellos.

11.3. Protección y ubicación de los equipos

11.3.1. Los usuarios no deben mover o reubicar los equipos de cómputo ni los de telecomunicaciones, ni instalar o desinstalar dispositivos, ni retirar sellos de los mismos sin la autorización de DTIC, en caso de necesitarlo, únicamente se requiere

que se envíe la solicitud al Director de DTIC, a través de un correo electrónico a atención.dtic@stj-sin.gob.mx, o bien, a su representante en la zona.

11.3.2. Administración de Bienes Informáticos de DTIC se encargará de elaborar los resguardos de los bienes informáticos, para ello, cuando a un usuario se le instale un bien informático, el Departamento de TIC´s de la región en la que fue instalado dicho bien, se encargará de recabar la firma del usuario, con esto, el usuario se acredita como el responsable de dicho activo y deberá conservarlos en la ubicación autorizada por DTIC o su responsable en la zona.

11.3.3. El equipo de cómputo asignado, deberá ser para uso exclusivo de las funciones que desempeña el empleado del Poder Judicial del Estado de Sinaloa.

11.3.4. 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 aprovechar al máximo las mismas.

11.3.5. 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, sistemas, utilerías informáticas, etc.

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

11.3.7. Se debe evitar colocar objetos encima del equipo o cubrir los orificios de ventilación del monitor o del gabinete, con el propósito de mantener el buen funcionamiento del equipo informático.

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

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

11.3.10. 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 Administración de Infraestructura Física, Servicios y Suministros de Oficialía Mayor a través de un plan detallado de movimientos debidamente autorizados por el titular del área que corresponda.

11.3.11. 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.

11.4. Mantenimiento de equipo informático

11.4.1. Únicamente el personal autorizado de DTIC o su representante en la zona 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.

11.4.2. 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 DTIC o su representante en la zona.

11.5. Mantenimiento preventivo de equipo informático

Los titulares de los Órganos Jurisdiccionales y/o Oficinas Administrativas, permitirán que el personal del Departamento de TIC´S de DTIC, o su representante en la zona, realicen el mantenimiento preventivo a los equipos informáticos con la finalidad de siempre conservar su continua disponibilidad e Integridad.

DTIC y/o el representante de ésta en la zona, enviarán un oficio al Órgano Jurisdiccional o Área Administrativa, en el cual informen la fecha en la que se llevará a cabo el mantenimiento preventivo a sus equipos. (Este se realizará preferentemente después de las 15:00 horas).

11.6. Eliminación Segura y/o reuso de equipo

Todas las computadoras, laptops y/o discos externos que contengan información almacenada y vayan a ser reasignadas a otro usuario o a otra adscripción distinta de la que actualmente se encuentra, deben ser revisadas por el usuario para que éste respalde su información, ya que cuando este equipo llegue a DTIC o con su representante en la zona, se realizará la eliminación de la información que contenía.

11.7. Desaparición, pérdida, robo o extravío de equipo de cómputo

11.7.1. 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.

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

11.7.3. En caso de desaparición, robo o extravío del equipo de cómputo o accesorios que estén bajo resguardo de un usuario, deberá dar aviso de inmediato a DTIC o al representante de éste en su zona, para iniciar el trámite interno e interponer la denuncia ante la autoridad competente.

11.8. Uso de dispositivos

11.8.1. El uso de los grabadores de discos compactos y/o dispositivos de almacenamiento tales como memorias usb,discos duros, etc. son exclusivos para respaldos de información que por su volumen así lo justifiquen.

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

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

11.8.4. El uso de cualquier dispositivo para conexión a internet privada deberá 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 DTIC.

11.9. 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, éste deberá cubrir el valor de la reparación o reposición del equipo o accesorio afectado. Para tal caso, DTIC determinará la causa de dicha descompostura.

12. TERCERA POLÍTICA GENERAL: "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 DTIC o ***su representante en la zona****, para solicitar asesoría.*

12.1. Uso de medios de almacenamiento

12.1.1. Cuando un empleado requiera usar o consultar la información que se tiene almacenada de otro compañero de la misma Área Administrativa u Órgano Jurisdiccional de trabajo, el Juez o el Titular del Área Administrativa enviará un correo electrónico a atención.dtic@stj-sin.gob.mx dirigido al Director de DTIC o al representante de ésta en su zona, donde:

- Explicará brevemente cuál es el fin de permitir compartir la información que se tiene en los medios de almacenamiento de un empleado a otro.
- Nombre y Puesto del empleado al que se le brindarán los derechos solicitados.

12.1.2. Los usuarios deberán respaldar de manera periódica la información sensitiva y crítica que se encuentre en sus computadoras personales o estaciones de trabajo, solicitando asesoría de DTIC o su representante en la zona, para que dichos asesores determinen el medio en que se realizará dicho respaldo.

12.1.3. En caso de que se requiera algún respaldo en CD debido a que se tiene mucha información sensible, este servicio deberá solicitarse desde la cuenta del Titular del Área a atención.dtic@stj-sin.gob.mx con atención al Director de DTIC.

12.1.4. 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, criterios y procedimientos institucionales para proporcionar a los particulares el acceso a la información pública que sea requerida al Poder Judicial del Estado de Sinaloa.

12.1.5. Para conservar la seguridad de la información, se llevará a cabo auditoría informática, es decir, se estarán realizando revisiones periódicas a las actividades informáticas que cada trabajador realiza, con la finalidad de detectar anomalías.

12.2. Instalación de Software que no es propiedad del Poder Judicial

12.2.1. 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 DTIC o al representante de ésta en su zona, enviando una solicitud a atención.dtic@stj-sin.gob.mx desde el correo electrónico del 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 DTIC o el representante de ésta en su zona, procederá de manera inmediata a desinstalar dicho software.

12.2.2. 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 DTIC, o al representante de ésta en su zona.

12.3. Identificación del incidente

12.3.1. El usuario que sospeche o tenga conocimiento de la ocurrencia de un incidente de seguridad informática deberá reportarlo a DTIC o al representante en

su zona, lo antes posible, indicando claramente los datos por los cuales lo considera un incidente de seguridad informática.

12.3.2. Cuando exista la sospecha o el conocimiento de que la 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.

12.3.3. 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 DTIC.

Dicho incidente se registrará en el Sistema Mesa de Ayuda Integral y un asesor se encargará de investigar la forma de solucionarlo.

12.4. 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 DTIC o su representante en la zona.

12.5. Seguridad para la red

Será considerado como un ataque a la seguridad informática y una falta grave, cualquier actividad no autorizada por DTIC o su representante en la zona, 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 operan sobre dicha red, con fines de detectar y mostrar una posible vulnerabilidad.

12.6. Uso del correo electrónico

12.6.1. 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 electrónico de alguien más (mientras esta persona se encuentra fuera o de vacaciones) 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.

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

12.6.3. 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 DTIC o su representante en la zona.

12.6.4. 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.

12.6.5. 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.

12.6.6. La asignación de una cuenta de correo electrónico externo, deberá solicitarse por escrito o enviar un correo electrónico a atención.dtic@stj-sin.gob.mx con atención al Director de DTIC, señalando los motivos por los que se desea el servicio. Esta solicitud deberá contar con el visto bueno del titular del área que corresponda, y en el caso de haber hecho la solicitud por medio de un correo electrónico, ésta deberá enviarse desde el correo del titular del área.

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

12.7. Controles contra código malicioso

12.7.1. 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 DTIC o representante de ésta en la zona.

12.7.2. Los usuarios del Poder Judicial del Estado de Sinaloa, deben verificar que la información y los medios de almacenamiento como: memorias USB, discos duros externos y CD´s, estén libres de cualquier tipo de código malicioso, para lo cual deben ejecutar el software antivirus autorizado DTIC o su representante en la zona.

12.7.3. El usuario debe verificar mediante el software de antivirus autorizado por DTIC o su representante en la zona 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.

12.7.4. 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.

12.7.5. 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 DTIC.

12.7.6. Cualquier usuario que sospeche de alguna infección por virus de computadora, deberá dejar de usar inmediatamente el equipo y llamar a DTIC o su representante en la zona, para la detección y erradicación del virus.

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

12.7.8. Los usuarios no deberán alterar o eliminar las configuraciones de seguridad para detectar y/o prevenir la propagación de virus que sean implantadas por DTIC en:

- Antivirus
- Outlook
- Office
- Navegadores u
- Otros programas.

12.7.9. 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 DTIC o su representante en la zona, para que sean ellos quienes solucionen esto.

12.8. Internet

12.8.1. 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.

12.8.2. La asignación del servicio de internet, deberá solicitarse por escrito a DTIC o también puede enviarse un correo-electrónico a atención.dtic@stj-sin.gob.mx, señalando los motivos por los que se desea el servicio. Esta solicitud deberá contar

con el visto bueno del titular del área correspondiente o deberá enviarse desde la cuenta de correo del titular del área correspondiente.

12.8.3. Todos los accesos a internet tienen que ser realizados a través de los proveedores de internet pagados por el Poder Judicial del Estado de Sinaloa.

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

12.8.5. El acceso a internet privada en el Supremo Tribunal de Justicia tiene que ser previamente autorizado por DTIC.

12.9. Obligaciones y/o monitoreo de usuarios que tienen el servicio de navegación en Internet

- 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 DTIC o su representante en la zona.
- 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.

12.10. Esquemas de permisos de acceso a internet y mensajería instantánea

Los esquemas de permisos de acceso a internet y 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 servicios de mensajería: Los usuarios podrán hacer uso de internet y servicios de mensajería instantánea, aplicándose las políticas de seguridad y navegación establecidas por el Departamento de Redes y Telecomunicaciones de DTIC.

NIVEL 3: Internet restringido y sin servicios de mensajería: Los usuarios sólo podrán hacer uso de internet aplicándose las políticas de seguridad y navegación establecidas por el Departamento de Redes y Telecomunicaciones de DTIC.

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

12.11. Internet libre

El Edificio del Supremo Tribunal de Justicia cuenta con servicio de internet libre, con la finalidad de brindar a sus visitantes la facilidad de consultar algunos datos desde sus celulares o cualquier dispositivo portátil.

12.12 Restricciones al conectar a la red del Poder Judicial del Estado de Sinaloa, cualquier equipo portátil propiedad del usuario

Está prohibido conectar a la red del Poder Judicial, laptops personales para realizar trabajo oficial, ya que cuando se solicita conectar una laptop que no es propiedad del Poder Judicial, se necesitarían recursos adicionales que permitan mantener segura la administración de las operaciones. (Licencias de antivirus, antimalware, antispam y antispyware), incrementar el ancho de banda, dando como resultado un decremento en la velocidad de respuesta tanto de los sistemas informáticos como en el uso de internet.

Asimismo, también se requiere instalación de nodos de red (este servicio está a cargo de Administración de Infraestructura Física, Servicios y Suministros de Oficialía Mayor del Supremo Tribunal de Justicia del Estado de Sinaloa).

13. CUARTA POLÍTICA GENERAL: "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, otorgándoles los permisos mínimos necesarios para el desempeño de sus funciones, con apego al principio "Necesidad del saber".

13.1. Controles de acceso lógico

13.1.1. Todos los consultores externos que realicen actividades de manera conjunta con el personal del Poder Judicial del Estado de Sinaloa en lo que respecta la

infraestructura tecnológica, requieren previamente obtener un permiso del Titular de Área del Poder Judicial del Órgano Jurisdiccional donde estarán brindando la asesoría especializada o desempeñando la actividad por la cual fueron contratados, posteriormente, el Titular de esa Área, enviará a DTIC o su representante en la zona, un oficio o un correo electrónico a atención.dtic@stj-sin.gob.mx atención al Director de DTIC, explicando:

- El motivo por el cual se les debe dar acceso a la infraestructura Tecnológica
- El tiempo que requiere el acceso lógico

13.1.2. 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.

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

13.1.4. 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 DTIC o su representante en la zona.

13.1.5. 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.

13.1.6. 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.

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

13.2. Administración de privilegios

13.2.1. Cambio de roles o responsabilidades de un empleado

Cualquier cambio que requiera hacerse a los roles y responsabilidades de algún empleado en la temática de privilegios de acceso a la infraestructura tecnológica del Poder Judicial del Estado de Sinaloa, el Titular del Área en la que esté adscrito el empleado, deberá solicitarlo desde su correo oficial a atención@stj-sin.gob.mx, dirigido al Director de DTIC.

13.3. Equipo desatendido

13.3.1. Activar protector de pantalla

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

13.3.2. Apagar computadoras y recursos tecnológicos cuando termina la jornada laboral

Los usuarios deben apagar sus computadoras u otros recursos tecnológicos cuando hayan terminado su jornada laboral diaria con la finalidad de proteger los equipos ante eventuales cortes de energía eléctrica.

13.4. Administración y uso de Passwords

13.4.1. 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.

13.4.2. Cuando un usuario olvide, bloquee o extravíe su contraseña deberá reportarlo por escrito a DTIC o su representante en la zona, o enviando un correo electrónico a atención.dtic@stj-sin.gob.mx, indicando si es de acceso a la red o a módulos de sistemas desarrollados por DTIC, para que se le proporcione una nueva contraseña.

13.4.3. La obtención o cambio de una contraseña debe hacerse de forma segura, el usuario deberá acreditarse ante DTIC o su representante en la zona, como empleado del Poder Judicial del Estado.

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

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

- No deben ser 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.

- Deben ser diferentes a las contraseñas (*passwords)* que se hayan usado previamente.

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

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

13.4.8. Los cambios o desbloqueo de contraseñas solicitados por el usuario a DTIC o su representante en la zona serán solicitados mediante oficio sellado y firmado por el jefe inmediato del usuario que lo requiere, o también se puede enviar un correo electrónico a atención.dtic@stj-sin.gob.mx con atención al Director de DTIC.

13.5. Control de accesos remotos

13.5.1. Está prohibido el acceso a redes externas por vía de cualquier dispositivo, cualquier excepción deberá ser documentada y contar con el visto bueno de DTIC o su representante en la zona.

13.5.2. 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 DTIC o su representante en la zona.

14.-QUINTA POLÍTICA GENERAL: "POLÍTICAS Y ESTÁNDARES DE CUMPLIMIENTO DE SEGURIDAD INFORMÁTICA

POLÍTICA:
De acuerdo al Reglamento Interior del Supremo Tribunal de Justicia del Estado de Sinaloa: "*La Dirección de Tecnologías de Información y Comunicaciones del Supremo Tribunal de Justicia tiene como una de sus funciones la de proponer y revisar el cumplimiento de normas y políticas de seguridad que garanticen acciones preventivas y correctivas para la salvaguarda de equipos e instalaciones de cómputo, así como de bancos de datos de información automatizada en general*.

14.1. Derechos de Propiedad Intelectual

13.1.1. 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.

13.1.2. Los sistemas desarrollados por personal interno o externo que controle DTIC o su representante en la zona, son propiedad intelectual del Poder Judicial del Estado de Sinaloa.

14.2. Revisiones del cumplimiento

14.2.1. DTIC o su representante en la zona, realizará acciones de verificación del cumplimiento del Manual de Políticas y Estándares de Seguridad Informática para usuarios.

14.2.2. DTIC o su representante en la zona, 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.

14.3. Violaciones de seguridad informática

14.3.1. Está prohibido el uso de herramientas de hardware o software para violar los controles de seguridad informática. A menos que se autorice por DTIC o su representante en la zona.

14.3.2. Está prohibido realizar pruebas de controles de los diferentes elementos de Tecnología de información.

Ninguna persona puede probar o intentar comprometer los controles internos a menos de contar con la aprobación de DTIC o su representante en la zona, con excepción de los Órganos Fiscalizadores.

14.3.3. 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 DTIC o su representante en la zona.

14.3.4. No se debe intencionalmente escribir, generar, compilar, copiar, coleccionar, propagar, ejecutar o introducir cualquier tipo de código (programa) conocidos como virus, gusanos o caballos de Troya, ó similares diseñado para autoreplicarse, dañar o afectar el desempeño o acceso a las computadoras, redes o información del Poder Judicial del Estado.

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

TÉRMINOS INFORMÁTICOS UTILIZADOS (GLOSARIO)

TÉRMINO	SIGNIFICADO
(A)	
Acceso	Tipo específico de interacción entre un sujeto y un objeto que resulta en el flujo de información de uno a otro. Es el privilegio de un sujeto para utilizar un objeto.
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, o bien usar.
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)	
Caballo de Troya	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.

Centros de cómputo, Centros de Procesamiento de datos o data center.	Es una Entidad, Oficina o Departamento que se encarga del procesamiento de datos e información de forma sistematizada. El procesamiento se lleva a cabo con la utilización de ordenadores que están equipados con el hardware y el software necesarios para cumplir con dicha tarea, estas computadoras se encuentran interconectadas en red.
Confidencialidad	Se refiere a que la información no sea divulgada a personal NO AUTORIZADO para su conocimiento.
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)	
Disponibilidad	Se refiere a que la información esté disponible en el momento que se necesite.
DTIC	Se refiere a la Dirección de Tecnologías de la Información y Comunicaciones del Supremo Tribunal de Justicia del Estado de Sinaloa.
Dominio	Sistema de denominación de host en internet. Conjunto de caracteres que identifica y diferencian los diferentes sitios.
Encriptación	Proceso matemático donde los datos de un mensaje, por seguridad, son codificados para protegerlos de accesos no deseados. El término encriptación como tal, no existe en el lenguaje español, el término correcto es CIFRADO DE DATOS.
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	Es la consecuencia que resulta del incumplimiento de la normatividad.
Free (Software libre)	Programas que se pueden bajar desde internet sin cargo.

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	Véase Caballo de Troya.
(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)	
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 o World Wide Web (www)	Es un sistema a nivel mundial de computadoras conectadas a una misma red, conocida como la red de redes 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.
(L)	
Lenguaje de Programación	Sistema de escritura para la descripción precisa de algoritmos o programas informáticos.
(M)	
Maltrato, descuido o negligencia	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.

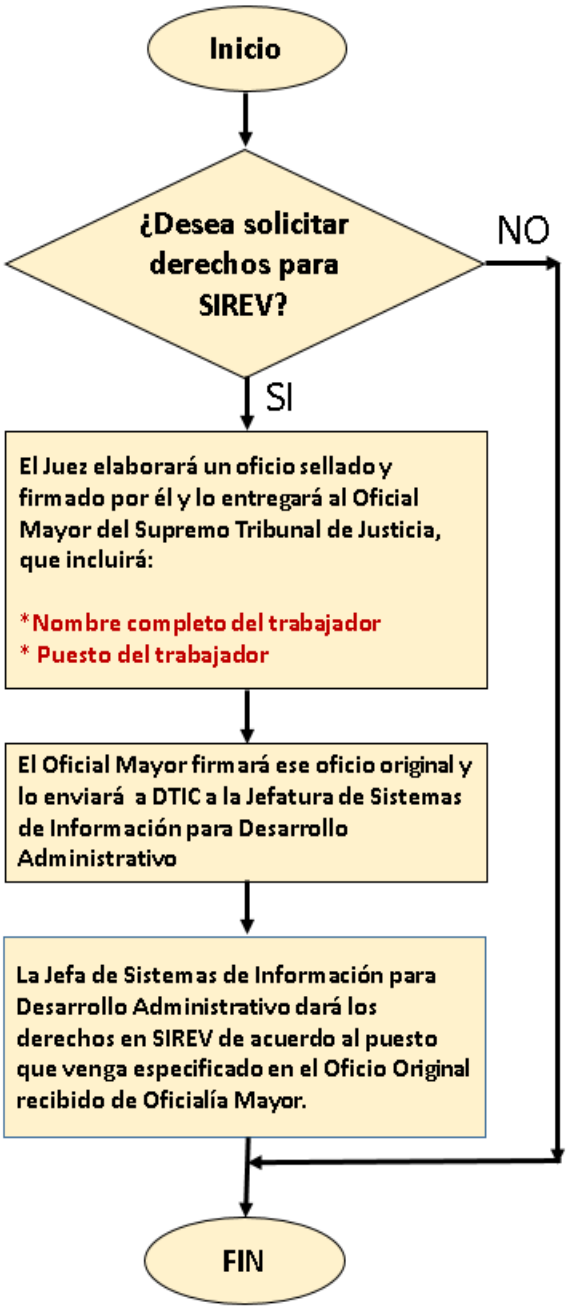
Mecanismos de seguridad o de control	Es un control manual o automático para proteger la información, activos tecnológicos, instalaciones, etc. que se utiliza para disminuir la probabilidad de que una vulnerabilidad exista, sea explotada, o bien ayude a reducir el impacto en caso de que sea explotada.
Medios magnéticos (medios de almacenamiento)	Son todos aquellos medios en donde se pueden almacenar cualquier tipo de información (diskettes, CD´s, DVD´s, etc.)
Metodología	Es un conjunto de procedimientos ordenados y documentados que son diseñados para alcanzar un objetivo en particular y comúnmente son divididos en fases o etapas de trabajo previamente.
Módem	Es un aparato electrónico que se adapta una terminal o computadora y se conecta a una red de comunicaciones (red telefónica). 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 o base	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.
Nodo	Punto principal en el cual se les da acceso a una red a las terminales o computadoras.
Normatividad	Conjunto de lineamientos que deberán seguirse de manera obligatoria para cumplir un fin dentro de una organización.
(P)	
Página Web	Ver sitio web.
Parche (patch)	Un parche (algunas veces llamado FIX) son piezas de programación que representan una solución rápida al software o sistema, para incrementar la funcionalidad del mismo.
Password	Contraseña. Secuencia de caracteres utilizados para determinar que un usuario específico requiere acceso a una computadora personal, sistema, aplicación o red en particular. Típicamente está compuesto de 6 a 10 caracteres.

(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.
Software Antivirus	Aplicaciones que detectan, evitan y posiblemente eliminan todos los virus conocidos, de los archivos ubicados en el disco duro y en la memoria de las computadoras.
Switch	Dispositivo de red que filtra y direcciona paquetes a las direcciones destinadas. El switch opera en la capa de enlace de datos del modelo OSI.
(T)	
Tarjeta inteligente	Es una tarjeta de plástico del tamaño de una tarjeta de crédito que incorpora un microchip, en el cual se puede cargar datos como números telefónicos, pagos realizados a través de medios electrónicos y otro tipo de aplicaciones, las cuales pueden ser actualizadas para usos adicionales.
(U)	
User-Id (identificación del Usuario)	Se denomina al nombre de usuario con el cual accedemos a una página o sistema en el que previamente nos hemos registrado. Este nombre puede estar compuesto de letras, número o signos.

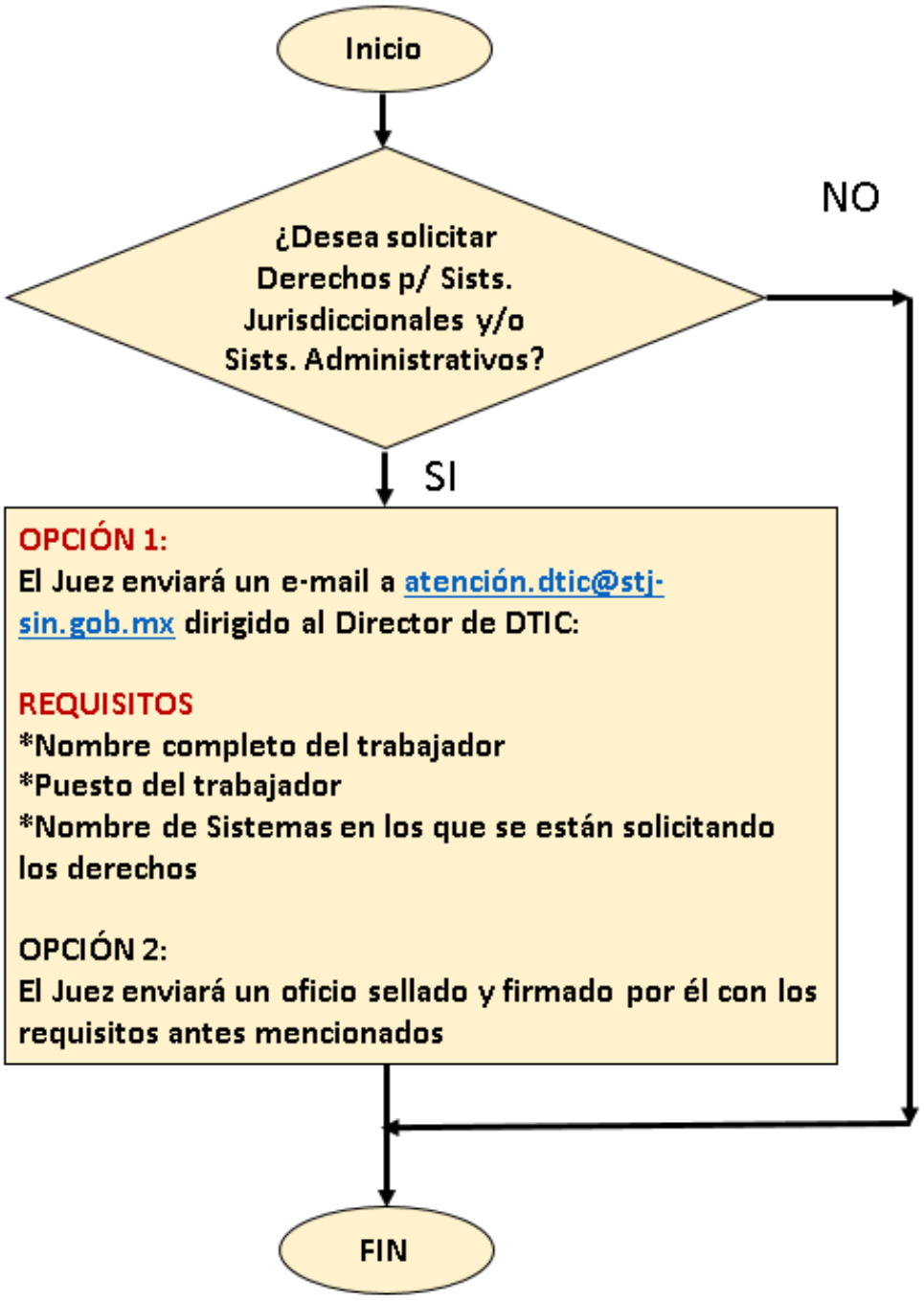
Usuario	Este término es utilizado para distinguir a cualquier persona que utiliza algún sistema, computadora personal o dispositivo (hardware).
(V)	
Virus	Programas o códigos maliciosos diseñados para esparcirse y copiarse de una computadora a otra por medio de los enlaces de telecomunicaciones o al compartir archivos o diskettes de computadoras.
Vulnerabilidad	Es una debilidad de seguridad o hueco de seguridad, el cual indica que el activo es susceptible a recibir un daño a través de un ataque, ya sea intencional o accidental.

15. DIAGRAMAS DE FLUJO:

15.1 Procedimiento cuando un empleado de nuevo ingreso requiera que se le asignen derechos en el Sistema SIREV (Sistema de Recepción y Entrega de Valores)



15.2 Procedimiento cuando un empleado de nuevo ingreso requiera que se le asignen derechos en Sistemas Jurisdiccionales y/o Administrativos



16. HISTORIAL DE VERSIONES:

Versión	Fecha	Comentario
1.0	28/09/2012	DTIC entregó el Manual de Políticas y Estándares de Seguridad Informática para usuarios del Poder Judicial a Secretaría Técnica para su revisión.
1.0	02/10/2012	Lo aprobó el H. Pleno del Supremo Tribunal de Justicia
1.0	07/08/2017 Al 25/09/2017	La Administradora de Proyectos y Estándares Tecnológicos realizó investigación de los nuevos cambios que hubo de ISO 27001:2005 A ISO 27001:2013 así como de las mejores prácticas de ISO 27002:2005 A ISO 27002:2015
2.0	30/10/2017	APyET* entregó la actualización de la Versión 1.0 a la Versión 2.0 del Manual de Políticas al Director para que él realizara las observaciones que considerara pertinentes.
2.0	22/11/2017	APyET* recibió las observaciones hechas por el Director de la Versión 2.0 del Manual que ella le entregó el día 30/Oct./18.
2.1	21/01/2018 Al 14/02/2018	APyET* realizó las observaciones hechas por el Director de la Versión 2.0 del Manual que recibió el 22/Nov./18 y generó versión 2.1.
2.1.	15/02/2018	APyET* entregó al Director el Manual Versión 2.1 que incluye las observaciones indicadas por él en fecha 22/Nov./17.
2.1.	06/04/2018	APyET* recibió las modificaciones que hizo el Director al Manual Versión 2.1 que ella le entregó el 15/Febrero/2018.
2.2.	06/04/2018	APyET* entregó al Director el Manual Versión 2.2. que incluye las observaciones indicadas por él en fecha 06/Abril/18.

***APyET= Administradora de Proyectos y Estándares Tecnológicos**