Política de uso aceptable de los recursos
de Tecnología de la Información
Poder Judicial de la Provincia de Santa Fe

1.- Consideraciones generales

a. El propósito de esta política es establecer las reglas y directrices para el uso aceptable del equipamiento informático que utilizan los usuarios en el Poder Judicial de Santa Fe. Esta reglamentación se aplica a Magistrados, Funcionarios, Agentes administrativos y a toda persona que haga uso de los sistemas de información y/o equipamiento propiedad del Poder Judicial. Este documento concentra las siguientes Normativas de la Corte Suprema de Justicia de la Provincia de Santa Fe sobre el tema: Acta 17/2002; Resolución 1648/2008; Circulares Nro. 19/2002, 06/2009, 84/2011, 12/2014, 54/2014, 8/2016, 19/2019, 92/2022, 93/2022, 5/2022, y 26/2023; las cuales conservan su vigencia.

b. Todos los usuarios de los sistemas de información son responsables de adherirse a esta política y de utilizar los recursos de manera ética, segura y legal.

c. El objetivo es generar una mayor concientización a los usuarios en aspectos de seguridad informática, a los efectos de transmitir la necesidad de cumplir con la reglamentación vigente y las recomendaciones en la materia. Todos los usuarios, deberán cumplir fehacientemente con la comunicación de incidentes de seguridad a la Secretaría Informática (por Teléfono, Correo, etc) informando los mismos tan pronto hayan tomado conocimiento de su ocurrencia. El equipo de seguridad informática del Poder Judicial será responsable de hacer cumplir estas normativas y tomar las medidas adecuadas en caso de faltas.

d.Se ordena la notificación formal de la presente a todos los integrantes de las unidades jurisdiccionales donde se encuentran instalados recursos informáticos.

1. e. Los recursos de tecnología de la información del Poder Judicial, incluidos las computadoras, redes, sistemas, software y datos, deben utilizarse únicamente para fines laborales legítimos y autorizados. Se prohíbe su uso para actividades ilegales, no éticas o inapropiadas, incluyendo, entre otras:

- Acceso no autorizado a sistemas o datos.
- Distribución de software pirata o ilegal.
- Creación, visualización o transmisión de contenido inapropiado, ofensivo o discriminatorio.
- Uso de los recursos informáticos para actividades personales no relacionadas con el trabajo. .
- Modificación no autorizada de configuraciones de seguridad o de software.

f. Hacer saber a los usuarios que son responsables del cuidado del equipamiento informático a su cargo, para el destino por el que le fuera provisto, no debiendo permitir su uso a personas extrañas a la unidad jurisdiccional al que fue asignado.

g. Establecer que la instalación de software en equipos de propiedad del Poder Judicial estará a cargo exclusivamente de la Secretaría de Informática o de terceros autorizados. Para casos de software especiales fundados en razones de servicio, siempre que no alteren las funcionalidades específicas, deberán contar con las licencias correspondientes y con autorización de las Secretarías de Gobierno y de Informática.

h. Hacer saber que los programas informáticos desarrollados por la Secretaría de Informática, son propiedad exclusiva del Poder Judicial y no podrán ser reproducidos ni utilizados por personal o ente alguno sin autorización previa de la Corte Suprema de Justicia. Los programas informáticos desarrollados por terceros y adquiridos por el Poder Judicial, sólo podrán ser utilizados por las unidades jurisdiccionales o dependencias judiciales a las que fueren asignados, estando prohibida su reproducción o utilización por persona o ente ajeno al mismo.

i. Hacer saber que los usuarios y contraseñas asignados para los sistemas son confidenciales y personales, identificando no sólo al usuario sino también su nivel de responsabilidad dentro de las tareas del Juzgado. Se aconseja, asimismo, cambiar la contraseña periódicamente, ante cualquier duda comunicarse con la Secretaría Informática.

j. Se recuerda que debe existir un usuario por computadora; y ante la necesidad de novedades, traslados o modificaciones, se lo debe comunicar con planilla correspondiente a la Secretaría de Informática.

k. Se subraya la importancia de la responsabilidad en el buen uso y mantenimiento del equipamiento informático, a cargo de la autoridad correspondiente de la Oficina. Se recomiendan controles especiales sobre los accesos a equipos con usuarios genéricos.

l. Los usuarios deberán comunicar a la Secretaría Informática, y al superior en su caso, de cualquier acontecimiento que considere, pudiere afectar la seguridad u operatividad del sistema informático.

m. La reparación de los desperfectos técnicos del equipamiento informático oficial instalado en las oficinas, será realizada exclusivamente por la Secretaría de Informática y por las empresas, contratadas específicamente para la prestación del soporte técnico o prestatarias de la garantía, quedando prohibida la intervención de personas ajenas.

n. Disponer que la Secretaría de Informática realice periódicamente auditorías sobre el hardware y software instalado en las oficinas judiciales, de propiedad del Poder Judicial, estando facultada a realizar los controles y verificaciones que correspondan para asegurar el cumplimiento de la presente normativa.

ñ. A efectos de resguardar el equipamiento, especialmente ante eventuales problemas eléctricos y accidentes, se reitera la necesidad de apagar diariamente todos los componentes que lo integran, Cpu, Monitor, Ups, y accesorios.

o. Asimismo se hace saber que en caso de donación de equipamiento

informático particular a este Poder Judicial y teniendo en cuenta la permanente renovación tecnológica, dicho equipamiento debe cumplir con las especificaciones técnicas necesarias para soportar todas las aplicaciones existentes y servicios que se brindan, como así también satisfacer requisitos de seguridad informática. Para tal fin se deberán comunicar con la Secretaría de Informática.

p. Sugerir a los titulares de cuentas de correo electrónico del dominio del Poder Judicial, que el envío y recepción de archivos lo efectúen a través del correo electrónico oficial con firma digital, debido a que cuenta con mayores medidas de seguridad, evitando el uso de periféricos móviles, tales como: pendrive, cd, dvd, fuentes de contaminación y propagación de virus. Para situaciones que excedan a este apartado, comunicarse con Secretaría de Informática.

q. Autorizar se disponga la máxima restricción en la utilización de puertos para conexión de dispositivos portables en puestos conectados a la red de servicios críticos. No se permitirá la conexión de teléfonos celulares y con respecto a los pendrive, los mismos deberán estar libres de virus y restringirse su uso a lo estrictamente necesario.

r. En caso de ser necesario la utilización de soportes de almacenamiento extraíbles (dispositivos USB, CD, DVD, discos externos, etc.), fuera del ámbito del PJSF, deberán considerarse aspectos tales como la autorización, el resguardo y el registro de los mismos, a fines de mantener su confidencialidad.

2. Consideraciones de seguridad a tener en cuenta para un uso correcto del correo electrónico:

a. Si bien el Poder Judicial posee soluciones de seguridad y antivirus tanto en los servidores perimetrales como internos y en las computadoras de todos los puestos, se recomienda un uso responsable del Correo electrónico.

b. Ser precavido a la hora de abrir correos de remitentes desconocidos, informando eventualmente a la oficina de Seguridad Informática. Generalmente

son intentos de phishing, cuyo objetivo es obtener datos del usuario, e incluyen un vínculo que parece dirigir al sitio oficial, pero en realidad lo llevan a un sito falso.

c. Sospechar de aquellos correos que tienen documentos adjuntos. En caso que en el adjunto vengan archivos (*.exe) o comprimidos (con extensión zip o rar, que soliciten una contraseña), se recomienda no abrirlos.

d. Verificación de remitente: Ante un correo sospechoso, situarse con el mouse sobre el texto de la cuenta de correo y revisarla, verificando que coincida con el texto observado. Ante alguna duda, comunicarse con la Secretaría de Informática.

e. Observar principalmente correos que sugieren abonar pagos o deudas, en otros idiomas o con caracteres desconocidos.

f. Ser cauteloso con los enlaces o links que se encuentran en el cuerpo del correo, nuevamente pasando el mouse por encima, para verificar que coincida con lo escrito.

g. Si se va a enviar correos a múltiples destinatarios, enviarlo como copia oculta para evitar la publicación de las direcciones de correo.

h. Tenga en cuenta que la Secretaría de Informática del PJSF nunca le solicitará que revele sus contraseñas o información personal vía e-mail, ni por páginas de internet referenciadas desde un correo.

i. Se solicita eliminar de las cuentas de correo electrónico oficiales, todos los mails que no guarden relación con el ámbito laboral y que puedan o no incluir fotos, imágenes, etc,

3.- Consideraciones en relación a los documentos de trabajo:

Todos los documentos de trabajo, deben almacenarse en la carpeta “Mis Documentos” (C:\documentos) para facilitar los procesos de backup que se realizan sobre dicha Carpeta y el resguardo de la información allí contenida. En dicha Carpeta solamente se deberán guardar documentos de carácter oficial y bajo ningún concepto se deben almacenar archivos ajenos al funcionamiento de

la dependencia judicial, especialmente: archivos de imágenes, música o video.

Tener especial cuidado con guardar Documentos en el escritorio de Windows; siempre se recomienda utilizar solamente accesos directos.

4.- Consideraciones de Seguridad relacionadas a la Navegación a Internet.

a. Facultar a la Secretaría de Informática la denegación del acceso a páginas y dominios de Internet que no estén relacionados con la actividad propia de cada oficina judicial.

b. Los equipos móviles, tipo notebook, celulares o módems, no están permitidos para su conexión a la red cableada del Poder Judicial. Si los mismos requieren acceso a Internet deberán utilizar la red Wifi correspondiente.

c. Para acceder a cualquier sitio web que por política de navegación no se pueda explorar desde las computadoras conectadas a la red troncal del Poder Judicial, se deben utilizar las conexiones WIFI, las computadoras de libre acceso ubicadas en sectores tribunalicios (ej: Bibliotecas), o si es esencial por razones de servicio, solicitar la autorización a la Secretaría de Gobierno; quién dará intervención a las áreas técnicas de la Secretaría de Informática.

d. Recordar que la dirección de los sitios en Internet seguros siempre comienzan con https://.

e. En caso que se acceda a Internet, a través de WIFI, con celulares o Notebooks, se deberá extremar el cuidado y la prevención, teniendo en cuenta que quedan registradas las direcciones IP del Poder Judicial.

5.- Acuerdo de Confidencialidad

Los agentes judiciales (cualquiera sea su situación de revista) que utilizan equipamiento informático del Poder Judicial, acuerdan la confidencialidad y no divulgación de la información a la que acceden. Asimismo, se comprometerán a utilizar la información solamente para el uso específico al que se ha destinado y a no comunicar, diseminar o de alguna otra forma hacerla pública a ninguna persona, empresa, o tercera persona, salvo autorización previa y escrita del

Responsable del equipamiento de que se trate.

Este requerimiento se aplica también a todos los proveedores que por razones de servicio tienen acceso al equipamiento informático del Poder Judicial.

6.- Política de protección de datos y Privacidad.

Se debe dar total cumplimiento a esta política emanada de un Plan de Seguridad, que establece los estándares y procedimientos para garantizar la privacidad y seguridad de los datos personales recopilados y procesados. Se debe tener un compromiso con la protección de la información confidencial de los usuarios y partes interesadas.

7.- Consideraciones sobre el incumplimiento:

Recordar que la violación o incumplimiento de la legislación y reglamentación vigentes de protección a la propiedad intelectual, aplicada a la instalación y uso del software y bases de datos, hará pasible al autor de la mismas de las sanciones penales previstas y disciplinarias que correspondieren, sin perjuicio de responder por los daños que causare a terceros y al Poder Judicial.

Se recuerda que el no cumplimiento de estas medidas podrá generar una investigación a los fines de evaluar las eventuales responsabilidades administrativas.

8.- Aplicación a terceros:

Esta reglamentación sera de aplicación tambien a toda persona que la Corte Suprema de Justicia autorice a realizar tareas que impliquen la utilización de los sistemas de información y/o del equipamiento propiedad del Poder Judicial. De la misma manera, si por razones de servicio, algún proveedor debe tener acceso a algún equipo informático y/o tecnologías con conexión a la red del Poder Judicial, también deberá cumplir las directivas presentes.

9. Estrategias de difusión:

Se determinará una amplia estrategia de difusión (capacitaciones, correos de concientización, sitio web, etc) para recordar las políticas de seguridad informáticas vigentes en el ámbito del Poder Judicial, advirtiéndose acerca de las consecuencias disvaliosas que trae aparejada el no cumplimiento de las mismas.