ACUERDO Nº 338.-: En la ciudad de San Luis a los VEINTISEIS días del mes de Mayo de Dos Mil Once, reunidos en la Sala de Acuerdos los Sres. Ministros del Superior Tribunal de Justicia: LILIA ANA NOVILLO; OMAR ESTEBAN URIA y OSCAR EDUARDO GATICA. Ausente los Sres Ministros HORACIO GUILLERMO ZAVALA RODRIGUEZ y FLORENCIO DAMIAN RUBIO.-

ACORDARON: I) APROBAR la Política de Seguridad de los Recursos Informáticos, que se transcribe a continuación:

Políticas de Seguridad de los Recursos Informáticos

1. OBJETIVOS:

En razón de que la información es un recurso que, como el resto de los activos, tiene valor para la Institución y por consiguiente debe ser protegida, la presente *Política de Seguridad de los Recursos Informáticos* tiene el propósito de gestionar adecuadamente la seguridad de la información, los sistemas informáticos y el ambiente tecnológico de los Organismos.

Estas políticas protegen los recursos de información del Poder Judicial y la tecnología utilizada para su procesamiento de una amplia gama de amenazas, internas o externas, deliberadas o accidentales, a fin de garantizar la integridad de los recursos informáticos que el Poder Judicial pone a disposición de los usuarios para el cumplimiento de sus tareas.

Es importante que los principios de la Política de Seguridad sean parte de la cultura organizacional, por lo tanto se debe asegurar un compromiso manifiesto de las máximas Autoridades de la Institución y de los jefes de oficinas para la difusión, consolidación y cumplimiento de esta política.

2. ALCANCE

El acceso a los diferentes sistemas de información y/o tecnologías informáticas que existen en el Poder Judicial conforman herramientas para mejorar la eficiencia en la prestación de las actividades y generan una correlativa responsabilidad a todos los usuarios de dichos elementos.

Por lo tanto, las políticas de seguridad deberán ser conocidas y cumplidas por toda la planta de personal de la Institución en todas sus circunscripciones, tanto se trate de personal judicial, administrativo o técnico, sea cual fuere su nivel jerárquico y su situación de revista que utilice elementos informáticos, cualquiera fuere la relación contractual que lo uniere con el organismo en el que se desempeña.

Se aplicará a la utilización tanto de los sistemas software, a los equipos informáticos (computadoras, impresoras, etc.), así como también a los recursos de la Red del Poder Judicial, más específicamente al acceso y operación de dicha red y al uso correcto de Internet (navegación, correo electrónico, etc.) cualquiera sea el horario en que se efectúe.

Cualquier situación que pudiere plantearse y que no se encuentre prevista en el presente reglamento, en razón de los continuos avances tecnológicos, quedará a consideración del Superior Tribunal de Justicia.

3. DISPOSICIONES GENERALES

Resulta necesario establecer una política de seguridad para proteger a los equipos de software poco confiable, especificando qué software está autorizado para ser ejecutado en una computadora, y prevenir la instalación no autorizada de software ilegal para el Poder Judicial.

3.1. Instalación de software y hardware

El software que deberá instalarse por defecto en todos los equipos del Poder Judicial es el siguiente:

Sistema Operativo.

Antivirus.

Suite de ofimática autorizada por la Secretaría de Informática Judicial (SIJ).

Cliente de Correo Electrónico para el acceso a cuentas de correo institucional.

Sistemas de Consultas de Jurisprudencia.

Sistemas de Gestión de Expedientes (GIAJ).

Software de soporte para firma digital.

Todo software o sistema desarrollado o autorizado por la SIJ.

Empleo de software y hardware adicional.

El usuario deberá hacer uso de una solicitud para la instalación de cualquier tipo de paquetes de software adicional o hardware requerido para su trabajo (ya sea provisto o personal). La instalación del software será efectuada por el personal informático dependiente de la SIJ, previa verificación de los requerimientos necesarios para su instalación y además del completo licenciamiento del mismo. Asimismo, deberá contarse con la correspondiente autorización de la SIJ y del responsable del organismo.

3.2. Cuentas de Usuario: Identificadores y contraseñas

El nombre de usuario (identificador) y su correspondiente contraseña proveen acceso a una cuenta de usuario de la red, del correo y de los sistemas del Poder Judicial y a los permisos asociados a ellas.

La contraseña no debe hacer referencia a ningún concepto, objeto o idea reconocible. Por tanto, se debe evitar utilizar en las contraseñas fechas significativas, días de la semana, meses del año, nombres de personas, teléfonos, etc, siendo el usuario totalmente responsable de esta.

En caso que el sistema no lo solicite automáticamente, el usuario debe cambiar la contraseña asignada la primera vez que realice un acceso válido al sistema, y se recomienda actualizarla en lapsos no mayores a 3 meses.

Las cuentas de usuario comunes no cuentan con los permisos necesarios para la administración de los equipos de trabajo instalado, es decir, únicamente les permite hacer uso de los programas comunes instalados en la computadora como son programas de oficina, sistema operativo y servicios básicos como impresión, correo, etc. Sólo el personal informático dependiente de la SIJ, puede realizar tareas propias de un administrador del equipo (configuración de dispositivos, agregar o quitar programas, agregar o eliminar hardware, etc.)

A todos los usuarios de red y equipos se les asignará un nombre normalizado y unificado.

4. POLÍTICAS de RESTRICCIÓN de los RECURSOS INFORMÁTICOS

4.1 Uso Aceptable

Se acepta que los usuarios aprovechen en forma limitada los elementos informáticos para un uso personal que derive en su mejor capacitación, jerarquización y/o especialización en sus conocimientos, prácticas y habilidades o para aprovechar los beneficios de la Informática.

El uso aceptable no podrá interferir con las actividades o funciones que el usuario cumple, ni con la misión y gestión oficial del organismo o dependencia.

Este uso personal podrá hacerse siempre que el recurso se encuentre disponible y no exista otro usuario que precise emplear el recurso para sus tareas laborales.

El uso aceptado no se considera un derecho del usuario y se encuentra sujeto al estricto control permanente de la autoridad de aplicación y de la autoridad del organismo donde el usuario desempeña sus funciones.

El uso aceptado puede ser controlado, revocado o limitado en cualquier momento por razón de la función, por cuestiones operativas y/o de seguridad de la Red ya sea por la autoridad de aplicación y/o por los funcionarios responsables del organismo.

No se considera uso aceptable aquel que demande un gasto adicional para el organismo, excepto el que derive del uso normal de los recursos informáticos.

Bajo ninguna circunstancia el uso de los recursos informáticos por parte de los usuarios deberá influir de manera negativa en el desempeño, la imagen, en las tareas o generar responsabilidades para el Poder Judicial.

4.2. Usos Indebidos

Se definen expresamente como *usos indebidos* los siguientes:

Modificar o reubicar equipos de computación, software, información, periféricos y/o cualquier otro medio de soporte de información (discos compactos, disquetes, cintas, etc.) sin la debida autorización de la Secretaría de Información Jurídica.

Modificar, alterar y/o borrar, sin las autorizaciones correspondientes, la información o las configuraciones de sistemas operativos o los aplicativos instalados por las personas autorizadas para tal efecto.

Transgredir o eludir las verificaciones de identidad u otros sistemas de seguridad;

Realizar cualquier actividad de recreación personal o de promoción de intereses personales (tales como creencias religiosas, hobbies, etc.) ;

Instalar o conectar cualquier equipamiento no autorizado;

Acceder al código fuente de una obra de software sin autorización explícita del autor (área de software y aplicaciones).

Alterar, falsificar o de alguna otra forma usar de manera fraudulenta los archivos, permisos, documentos de identificación, u otros documentos o propiedades;

Leer información o archivos de otros usuarios sin su permiso;

Difundir indebidamente y/o indiscriminadamente la información privada o pública a que tuviere acceso con motivo de la función o actividad que desempeña;

Intentar obtener otros derechos o accesos distintos a aquellos que les hayan sido asignados.

Intentar acceder a áreas restringidas de los Sistemas de Información.

Intentar distorsionar o falsear los registros de los Sistemas de Información.

Intentar descifrar las claves, sistemas o algoritmos de cifrado y cualquier otro elemento de seguridad que intervenga en los procesos.

Poseer, instalar, desarrollar o ejecutar programas que pudieran interferir sobre el trabajo de otros Usuarios, o dañar o alterar los Recursos Informáticos.

Los usuarios tendrán acceso autorizado únicamente a aquellos datos y recursos que precisen para el desarrollo de sus funciones, conforme a los criterios establecidos por el responsable del organismo.

Todo el personal que accede a los Sistemas de Información del Poder Judicial debe utilizar únicamente las versiones de software facilitadas por

personal autorizado del área competente y siguiendo sus normas de utilización.

4.3. Usos Prohibidos

La sustracción de equipos o periféricos informáticos, y/o cualquier otro medio de soporte de información (discos compactos, disquetes, cintas, etc.) constituye un delito de acción pública.

Se encuentra expresamente prohibido el uso de la Red o de cualquier recurso informático que infrinja normas nacionales o provinciales, causen daño o perjudiquen al Poder Judicial o a terceros.

Se encuentra especialmente *prohibido el uso* de cualquier recurso informático para:

Grabar, modificar o borrar software, información, bases de datos o registros del Poder Judicial, que no estén incluidas como tareas propias del usuario.

Inferir cualquier daño a los equipos o a la información, las configuraciones de sistemas operativos o los aplicativos que se encuentren en ellos instalados;

Acceder sin autorización a los sistemas de información de los diferentes organismos;

Obtener cualquier tipo de ganancia económica personal;

Revelar o compartir contraseñas de acceso, propias o de terceros, con otros usuarios así como el uso de la identificación, identidad, firma electrónica o digital de otro usuario;

Enviar cualquier transmisión de datos en forma fraudulenta;

Introducir en los Sistemas de Información o la Red contenidos obscenos, amenazadores, inmorales u ofensivos;

Utilizar cualquier sistema de correo o cualquier tipo de comunicación electrónica con el propósito de revelar información privada de otras personas, sin su consentimiento;

Utilizar cualquier sistema de correo electrónico o cualquier tipo de comunicación electrónica con el propósito de dañar o perjudicar de alguna manera los recursos informáticos;

Lanzar cualquier tipo de virus, gusano, macros, applets, controles ActiveX o cualquier otro dispositivo lógico o secuencia de caracteres cuya intención sea hostil, destructiva, o que afecte directamente en el funcionamiento adecuado de los diferentes sistemas y recursos informáticos;

Lanzar, activar, ejecutar o permitir cualquier tipo de software o hardware que genere una degradación o denegación de cualquiera de los servicios o activos informáticos.

Realizar cualquier actividad contraria a los intereses del Poder Judicial, tal como publicar información reservada, acceder sin autorización a recursos o archivos o impedir el acceso a otros usuarios mediante el mal uso deliberado de recursos comunes;

Alterar, falsificar o de alguna otra forma usar de manera fraudulenta los archivos, permisos, documentos de identificación u otros documentos o propiedades;

Acceder, descargar, transmitir, distribuir o almacenar videos, música, imágenes, documentos y/o cualquier otro software o archivo cuya finalidad no se ajuste a la responsabilidad laboral de las funciones conferidas al agente;

Violar cualquier ley o norma provincial o nacional, respecto al uso de los sistemas de información así como también realizar cualquier conducta ilegal

contraria a la legislación aplicable de cualquier país al que se pueda tener acceso por la Red.

4.4. Responsabilidades

Ningún usuario debe usar la identificación, identidad, firma electrónica, firma digital o contraseña de otro usuario, aunque dispongan de la autorización del propietario.

Los usuarios de la red deben tomar los recaudos y la precaución para mantener su cuenta segura, es decir que no deben revelar bajo ningún concepto su contraseña o identificación a otro, a excepción de casos que deban facilitarse para la reparación o mantenimiento de algún sistema o equipo. En este caso y en forma estrictamente circunstancial, sólo deberá hacerlo al personal técnico o informático debidamente identificado, con la posibilidad que posteriormente dicho agente solicite al área técnica responsable, la modificación de claves, contraseñas u otro tipo de elemento de seguridad que implique riesgo de acceso por un tercero a los diferentes sistemas de información.

Si un usuario tiene sospechas de que su acceso autorizado (identificador de usuario y contraseña) está siendo utilizado por otra persona, debe proceder al cambio de su contraseña y contactar con la SIJ para notificar la incidencia.

Es responsabilidad del usuario el cuidado y buen trato de los recursos informáticos asignados.

4.5. Derechos y Deberes de los usuarios

Son *derechos* de los usuarios:

Recibir ayuda y asesoramiento por parte del personal del servicio técnico correspondiente.

Formular las sugerencias que estimen oportunas para mejorar el servicio.

Disponer de los recursos provistos por el Poder Judicial, dentro de las normas correspondientes, para la gestión y la carga de trabajo asignados.

Acceder a información relacionada con su función.

Utilizar el correo electrónico, listas de discusión y otros servicios, locales o de internet, siempre que tengan relación directa con la función del usuario en el organismo.

Utilizar los recursos informáticos en forma limitada para su capacitación, sin que dicho uso interfiera con las actividades o funciones que el usuario cumple, ni con la misión y gestión oficial del organismo o dependencia.

Acceder a los cursos de capacitación y actualización que los Organismos implementen en función de las actividades y labores que los usuarios desarrollen.

Utilizar los recursos informáticos de conformidad con las presentes normas.

Son *deberes* de los usuarios:

Notificar al personal informático de los cambios de funciones dentro del mismo organismo, o su traslado a otro, a fin de asignarle nuevos permisos o nuevos sistemas según corresponda.

Contribuir al cuidado y conservación de las instalaciones, equipos y sistemas.

Notificar al personal del servicio técnico de las anomalías que se detecten, tanto de software como de hardware.

Respetar las indicaciones que reciban de los responsables de cada área respecto al uso y funcionamiento de los equipos.

El cumplimiento de las normas y condiciones establecidas en la presente normativa.

5. USO ESPECÍFICO DE INTERNET

Queda autorizado el uso del servicio de acceso a Internet para Magistrados y Funcionarios del Poder Judicial cualquiera sea la función que desempeñen, y siempre que aquel esté directamente relacionado con ésta. Sólo se permitirá el acceso a los dominios de primer nivel que contengan información de gobierno, organizaciones sin fines de lucro, académicas, de investigación y educativas (gov, net, org, edu, com, etc.).

Sólo se permitirá el uso restringido de Internet al personal administrativo. Cuando sea necesario que personal administrativo haga uso de un servicio o dominio adicional, ello será solicitado por el responsable del área correspondiente indicando el motivo y/o beneficio para el servicio de justicia. La petición será dirigida a la SIJ.

La SIJ tomará los recaudos técnicos necesarios para filtrar los accesos a los dominios no autorizados.

Régimen del correo electrónico:

Todo Magistrado, Funcionario y Empleado podrá acceder a una "cuenta oficial personal" de correo electrónico, y a una "cuenta oficial institucional" en la medida que sea necesario funcionalmente y posible materialmente.

Si bien el uso de las "cuentas personales", se rige por un principio de apertura y libertad en las comunicaciones, estas no deberán ser contrarias, o reñidas con el carácter de público estatal y judicial que le proporciona el dominio justiciasanluis.gov.ar, que identifica al Poder Judicial de la Provincia de San Luis.

Todas las Unidades Funcionales poseerán una "cuenta institucional" de correo, la que está destinada a las comunicaciones formales entre

organismos y/o entidades judiciales y no judiciales de la jurisdicción provincial, como así también de otras jurisdicciones provinciales, nacionales o extranjeras que acepten este método de comunicación electrónica. Esta podrá ser utilizada conjuntamente con el procedimiento informático de "Firma Digital", conforme a las leyes vigentes, mediante el cual se proporciona seguridad sobre la autoría, veracidad e integridad al documento transmitido.

Todas la comunicaciones que se realicen mediante equipamiento de propiedad del Poder Judicial, servicios de comunicaciones contratados y cuentas de correo administradas por éste, deberán tener por objetivo directo o indirecto, el mejor Servicio de Justicia.

6. POLÍTICAS de SEGURIDAD FÍSICA y AMBIENTAL

6.1 Control de acceso físico

Los responsables de los equipos deberán controlar y limitar el acceso a las instalaciones de procesamiento de información, exclusivamente a las personas autorizadas.

6.2 Ubicación y protección del equipamiento informático

El equipamiento será ubicado y protegido de tal manera que se reduzcan los riesgos ocasionados por amenazas y peligros ambientales, y las oportunidades de acceso no autorizado, teniendo en cuenta los siguientes puntos:

Ubicar el equipamiento en un sitio donde se provea un control de acceso adecuado (puertas con cerraduras, ventanas con trabas, etc.).

Adoptar controles adecuados para minimizar el riesgo de amenazas potenciales por: robo o hurto, incendio, humo, polvo, vibraciones, inundaciones o filtraciones de agua, efectos químicos, radiación electromagnética, derrumbes, interferencia en el suministro de energía

eléctrica (cortes de suministro, variación de tensión). En este último caso, desconectar de la alimentación principal únicamente el equipamiento y esperar hasta el restablecimiento normal de la misma. Nunca desconectar ninguna ficha del gabinete estando encendido el equipo.

Revisar regularmente las condiciones ambientales para verificar que las mismas no afecten de manera adversa el funcionamiento del equipamiento informático.

6.3 Mantenimiento del equipamiento informático

Sólo personal autorizado y calificado, dependiente de la SIJ puede brindar mantenimiento y llevar a cabo reparaciones en los equipos y/o periféricos informáticos.

En el caso de que la reparación implique el formateo y/o reemplazo de disco rígido, el usuario deberá realizar previamente las respectivas copias de resguardo, salvo en el caso de que dicho dispositivo se encuentre inutilizado, y sea imposible realizarlas.

6.4 Copias de Seguridad de la información

Los usuarios podrán solicitar, cuando lo consideren necesario, la realización de copias de resguardo de la información sensible o crítica para el Organismo. Este requerimiento deberá ser efectuado al personal técnico dependiente de la SIJ.

6.5. Políticas de Escritorios y Pantallas Limpias

Se deberá adoptar una política de escritorios limpios para proteger los dispositivos de almacenamiento removibles y una política de pantallas limpias en los equipos informáticos, a fin de reducir los riesgos de acceso no autorizado, pérdida y daño de la información, tanto durante el horario normal de trabajo como fuera del mismo.

Se aplicarán los siguientes lineamientos:

a) Almacenar en un mobiliario seguro bajo llave, cuando corresponda, los medios informáticos con información sensible o crítica del Organismo, cuando no están siendo utilizados, especialmente fuera del horario de trabajo.

b) Evitar dejar abiertos documentos, unidades de almacenamiento de datos y sesiones sistemas informáticos, en el caso de ausentarse del puesto de trabajo con el fin de preservar y garantizar la integridad y seguridad de los mismos.

c) Retirar inmediatamente la información sensible o confidencial, una vez impresa.

6.6. Ingreso y Retiro de bienes informáticos

La introducción de cualquier equipo o periférico informático ajeno al Poder Judicial, no podrá realizarse sin previa autorización de la Secretaria de Informática Judicial.

Cualquier equipo o periférico informático perteneciente al Poder Judicial, como así también aquellos ajenos al mismo pero que están autorizados a funcionar, no podrán ser retirados de la sede del Organismo sin autorización formal.

7. OTRAS RESTRICCIONES

7.1 Asistencia Informática

Los usuarios deberán canalizar las peticiones de asistencia o soporte técnico al Departamento Técnico, dependiente de la SIJ.

7.2 Monitorización

Los usuarios que utilicen equipos del Organismo para acceder a la red e Internet están sujetos a ser monitoreados, en sus actividades por personal de sistemas o redes, autorizado a tal efecto. Dicha tarea se realizará a través de los mecanismos formales y técnicos que se consideren oportunos, ya sea de forma periódica o cuando por razones específicas de seguridad o del servicio resulte conveniente, con el fin de velar por el correcto uso de los mencionados recursos.

El simple uso de los servicios de Red implica el consentimiento a este monitoreo por cuestiones operativas o de seguridad, debiendo los empleados tener en cuenta que la mayoría de las sesiones no son privadas.

La información personal del Usuario a la que se tenga acceso como consecuencia de las actividades de control, mejor funcionamiento o seguridad, no podrá ser difundida públicamente excepto que se trate de un uso no autorizado, indebido o prohibido y a los estrictos fines de iniciar la pertinente denuncia administrativa y/o judicial.

8. TÉRMINOS y DEFINICIONES

Seguridad de la Información que se entiende como la preservación de:

• Confidencialidad: se garantiza que la información sea accesible sólo a aquellas personas autorizadas a tener acceso a la misma.

• Integridad: se salvaguarda la exactitud y totalidad de la información y los métodos de procesamiento.

• Disponibilidad: se garantiza que los usuarios autorizados tengan acceso a la información y a los recursos relacionados con la misma, toda vez que lo requieran.

Legalidad: referido al cumplimiento de las leyes, normas, reglamentaciones o disposiciones a las que está sujeto el Organismo.

Confiabilidad de la Información: es decir, que la información generada sea adecuada para sustentar la toma de decisiones y la ejecución de las misiones y funciones.

Información: Se refiere a toda comunicación o representación de conocimiento como datos, en cualquier forma, con inclusión de formas textuales, numéricas, gráficas, cartográficas, narrativas o audiovisuales, y en cualquier medio, ya sea magnético, en papel, en pantallas de computadoras, audiovisual u otro.

Sistema de Información: Se refiere a un conjunto independiente de recursos de información organizados para la recopilación, procesamiento, mantenimiento, transmisión y difusión de información según determinados procedimientos, tanto automatizados como manuales.

Tecnología: Se refiere al hardware y software operados por el Organismo o por un tercero que procese información en su nombre, para llevar a cabo una función propia del Organismo, sin tener en cuenta la tecnología utilizada, ya se trate de computación de datos, telecomunicaciones u otro tipo.

Activos:

• Recursos de información: bases de datos y archivos, documentación de sistemas, manuales de usuario, material de capacitación, procedimientos operativos o de soporte, planes de continuidad, información archivada, etc.

• Recursos de software: software de aplicaciones, sistemas operativos, herramientas de desarrollo, utilitarios, etc.

• Activos físicos: equipamiento informático (procesadores, monitores, computadoras portátiles, módems), equipos de comunicaciones (routers, PABXs, máquinas de fax, contestadores automáticos), medios magnéticos (cintas, discos), otros equipos técnicos (relacionados con el suministro

eléctrico, unidades de aire acondicionado), mobiliario, lugares de emplazamiento, etc.

• Servicios: servicios informáticos y de comunicaciones, utilitarios generales (calefacción, iluminación, energía eléctrica, etc.).

Usuario: Todas aquellas personas físicas o de existencia ideal que utilicen sistemas, software, activos y los servicios de Red provistos por el Poder Judicial.

9. FUENTES NORMATIVAS CONSULTADAS

"*Modelo de Política de Seguridad de la Información para Organismos del Sector Público Nacional*" (Versión 1, Julio-2005), aprobada por la Oficina Nacional de Tecnologías de Información (ONTI) de La Subsecretaría de Gestión Pública de la Jefatura de Gabinetes de Ministros.

"Régimen sobre el Uso Responsable de Elementos Informáticos", en el ámbito del Poder Ejecutivo de la Provincia de Buenos Aires. Aprobado por Decreto N°2442, el 12 de Oct. 2.005. (Publicación B.O., 9 Nov. 2.005).

Normas y recomendaciones de la Coordinación de Emergencias en redes Teleinformáticas de la Administración Pública Argentina (ArCERT)

"*Política Institucional y Procedimiento para el Uso Ético Legal de las Tecnologías de Información de la Universidad de Puerto Rico***"** (Universidad de Puerto Rico en Bayamón - 1999/2000).

"*Políticas de Seguridad de los Recursos Informáticos del Poder Judicial de Santiago del Estero*".

"*Resolución Administrativa 301/2002*" - Poder Judicial del Chubut

Con lo que se dio por terminado el presente acto, disponiendo los Señores Ministros se comunique a quienes corresponda, firmando ante mí, doy fe.-