ADM 2134/16

PROTOCOLO DE ACUERDOS 2017

ACUERDO N° 61: En la Provincia de San Luis a VEINTICUATRO días del mes de FEBRERO de DOS MIL DIECISIETE, los Señores Ministros del Superior Tribunal de Justicia Dres. OMAR ESTEBAN URÍA, HORACIO GUILLERMO ZAVALA RODRÍGUEZ y LILIA ANA NOVILLO.-

DIJERON: Que por Acuerdo N° 386/2012, registrado en la Dirección Nacional de Derecho de Autor (Expte. Nº 5057487, 30/10/2012) se estableció la primera reglamentación General de Uso del Sistema de Gestión Informático, que se iría enriqueciendo con el avance del proceso de despapelización, en la medida que resultara necesario, con la formalidad de Texto Ordenado, de manera de facilitar el acceso de los interesados obteniendo siempre un texto único, completo y vigente, que sea la referencia autosuficiente para las consultas relacionadas con el expediente electrónico en uso.-

Que el avance alcanzado en el presente en el mencionado proceso, nos posiciona en condiciones de ser el primer Poder Judicial del País que tramita todos los expedientes en soporte electrónico y sin respaldo papel. Que esta modalidad de trabajo implica la necesidad de contar con una normativa novedosa que dé sustento formal a una práctica forense sin antecedentes.

Así, en ese proceso de actualización se llegó por Acuerdo Nº 263/2015 (modificado por Acuerdo Nº 325/2015) al último Reglamento General de Expediente Electrónico, que debió ser revisado para contemplar un escenario de despapelización total.

Que en consecuencia se han considerado, en las modificaciones que se introducen, las necesidades surgidas de la experiencia en el uso del sistema de gestión informático y en la despapelización comenzada en el año 2014. Esas modificaciones versan sobre puntos sustanciales del trámite del expediente como ser: ingreso de nuevas causas y primer escrito, funciones de Mesa General Única, verificaciones de créditos, Registro de Juicios Universales, recursos de queja, comunicaciones electrónicas, oficios y exhortos Ley 22.172, notificación ficta,

sumario de prevención, plazo de gracia, control de gestión, auditorías y audiencias de prueba.-

Que, por otra parte, y de conformidad a lo ordenado por Acuerdo Nº 213/2016 se han analizado los Acuerdos 423/1990, 860/2010, 270/2012, 49/13, 794/2013, 321/14, 394/2014, 468/2014, 202/2015, 263/2015, 280/2015, 325/2015, 335/2015, 422/2015, 423/2015, 507/2015 y 238/2016.-

Por ello y en virtud de lo dispuesto por Ley Nacional Nº 25.506, Ley Nº V-0591-2007, Ley Nº V-0699-2009, y atribuciones reglamentarias otorgadas por ésta última y por la Ley Orgánica de Administración de Justicia en su art. 42, inc. 4;

ACORDARON:

I.- APROBAR el nuevo texto ordenado del REGLAMENTO GENERAL DE EXPEDIENTE ELECTRÓNICO, cuyo índice y contenido se agregan como Anexo del presente Acuerdo, el que integrará el nuevo DIGESTO DIGITAL DE ACORDADAS (Acuerdos 201/2015, 421/2015 y 213/2016).-

II.- DISPONER que el presente Acuerdo será de aplicación a partir de su publicación para todos los Organismos del Poder Judicial, a excepción de los Juzgados de Instrucción y de Sentencia y Cámaras del Fuero Penal, Correccional y Contravencional de la Primera y Segunda Circunscripción, para los cuales será aplicable a partir del día 3 de abril de 2017 fecha a partir de la cual quedará despapelizado todo el Poder Judicial, rigiendo inter a su respecto el Acuerdo Nº 263/2015.-

III.- DEJAR SIN EFECTO los ACUERDOS Nº 423/1990, 860/2010, 270/2012, 49/13, 794/2013, 321/14, 394/2014, 468/2014, 202/2015, 263/2015, 280/2015, 325/2015, 335/2015, 422/2015, 423/2015, 507/2015 y 238/2016 y toda otra disposición que se oponga al presente.-

IV.- ORDENAR LA PUBLICACIÓN DEL PRESENTE ACUERDO POR UN DÍA EN EL BOLETIN OFICIAL Y JUDICIAL DE LA PROVINCIA Y EN EL SITIO WEB DEL PODER JUDICIAL, Y LA REGISTRACIÓN EN EL REGISTRO DE AUTORES. -

Con lo que se dio por finalizado el acto, disponiendo los Sres. Ministros se comunique a quienes corresponda.-SIJ

INDICE TEMÁTICO

REGLAMENTO GENERAL EXPEDIENTES ELECTRÓNICO

REGLAMENTO GENERAL DE EXPEDIENTE ELECTRÓNICO:

TÍTULO I

PRINCIPIOS GENERALES

CAPÍTULO I

DATOS. SEGURIDAD. SERVICIO

ART. 1. VALIDEZ DE LAS CONSTANCIAS DE LOS EXPEDIENTES:

Las constancias de datos, libros, movimientos (radicación, elevación, vista, eventos, pases, etc.) y todos los documentos que conforman el expediente electrónico no se imprimirán y serán consideradas válidas sin necesidad de respaldo papel, en todos los fueros e instancias.

ART. 2. REGISTRO DE DATOS EN EL SISTEMA:

Es de práctica obligatoria la carga y el control diario y permanente de la información en el sistema informático de todo lo producido en cada organismo judicial. Los responsables funcionales de los expedientes deberán asegurar y controlar la carga íntegra y autosuficiente de datos en el expediente electrónico, a fin de que contenga todas las actuaciones y movimientos del proceso, firmando digitalmente aquellas en las que intervengan. También asegurarán el asiento completo y oportuno de los datos que correspondan para conformar en soporte electrónico los Libros de Secretaría que establecen las leyes y reglamentos.

Se prestará especial atención a la correcta carga de datos de todos los sujetos involucrados en los expedientes, con sus datos identificatorios inequívocos (DNI, CUIL, CUIT, domicilio, Representante, etc.), como así a los datos de los domicilios postales y electrónicos constituídos en el expediente.

Los Secretarios y los Funcionarios de Ministerios Públicos en su caso, serán responsables de mantener actualizada la carga de información, de controlar eficazmente la oportunidad y completitud de la información cargada en el sistema informático en sus respectivos organismos, y de asegurar la correcta vinculación de las partes para posibilitar la visualización de las causas por vías electrónicas.

ART. 3. IDENTIFICACIÓN DE LOS JUSTICIABLES:

Todo escrito de presentación inicial en cada expediente deberá contener la correcta individualización de las partes peticionantes: las personas físicas con el DNI, CUIT o CUIL y las jurídicas con el CUIT, como condición necesaria y excluyente para ser proveídas las peticiones que contenga. Será obligación de los Sres. Abogados y de los justiciables en general, aportar los datos correspondientes a su parte con el debido respaldo (fotocopia del DNI y constancia de CUIT, según el caso), a efectos de asegurar la exactitud de los datos personales en la base correspondiente. El requisito de identificación descripto se exigirá para dar de alta en sistema a los testigos al momento de declarar.

En caso de que se presenten ciudadanos sin patrocinio letrado a radicar una denuncia, será indispensable la acreditación de su identidad ante el funcionario actuante.

ART. 4. ALTA DE PERSONAS:

Cuando al momento de ingresar una persona en una causa judicial, agotadas todas las opciones de búsqueda que ofrece el sistema informático, no se encuentren los datos del justiciable a ingresar, el alta de esta nueva persona en la base de datos del sistema será efectuado exclusivamente por las personas y dependencias autorizadas. Los autorizados serán personalmente responsables de la carga que efectúen.-

ART. 5. IDENTIFICACIÓN DE EXPEDIENTES:

Los expedientes que se ingresen al sistema informático recibirán un número de identificación único, que no podrá ser cambiado por otro hasta su destrucción, sin importar los cambios de radicación o elevaciones que ocurran durante su vida útil. Si por algún motivo se autorizara una nueva numeración, deberá asegurarse la posibilidad de buscar por el número originario.

Cuando, por resolución fundada, se decida dar de baja del sistema de gestión un expediente, se comunicará tal decisión por Oficio a Secretaría de Informática, para que proceda de conformidad.

ART. 6. CASILLA DE CORREO INSTITUCIONAL:

Es obligatoria la consulta diaria del correo electrónico recibido en las casillas institucionales.

Será responsabilidad de cada usuario, evitar la sobrecarga de las distintas bandejas de sus casillas de correo, de manera que estén siempre en condiciones de recibir nuevas comunicaciones. Secretaría de Informática Judicial auditará periódicamente el cumplimiento de esta obligación.

La falta de recepción de notificaciones electrónicas no podrá alegarse válidamente, para impedir el efecto propio de los plazos procesales, cuando medie incumplimiento de esta obligación. Por lo tanto, quien emita o recepte un documento, si desea conservarlo, deberá guardarlo localmente en su computadora.

ART. 7. PROTOCOLOS:

Se considera cumplida la obligación de protocolizar copias fieles de las sentencias definitivas e interlocutorias, con la existencia de los documentos firmados digitalmente que las contienen y que obren en la base de datos del sistema informático.

ART. 8. CORTES DEL SERVICIO INFORMÁTICO:

En los casos de cortes en el sistema informático las obligaciones impuestas en el presente Reglamento, deberán cumplirse una vez que el servicio se restablezca, ya sea en horario hábil o inhábil si fuera necesario.

Durante los cortes, toda audiencia, decreto y actuación judicial que pueda concretarse se generará en procesador de texto localmente y las actuaciones así producidas, deberán incorporarse al sistema informático al restablecerse el servicio. En caso de que la audiencia fuera de absolución de posiciones y no se

contara con el documento del pliego, se suspenderá la audiencia y en el mismo acto se fijará nueva fecha.
Cuando la gravedad y duración del corte de servicio lo amerite, el Superior Tribunal dispondrá la suspensión de los términos procesales.

ART. 9. FIRMA DE LAS ACTUACIONES.
Atento el efecto propio de la Firma Digital previsto por las leyes, queda sin efecto el requisito de la firma del Secretario rubricando o certificando la firma del Magistrado en todas las actuaciones generadas en el sistema informático.
En todas las actuaciones que se firmen digitalmente deberá indicarse al pie el nombre y cargo del firmante de las mismas.

ART. 10. USO INDEBIDO DEL DISPOSITIVO CRIPTOGRÁFICO.
En caso de detectarse que los dispositivos criptográficos (Token) están siendo utilizados por Magistrados, Funcionarios y Empleados judiciales que no sean los titulares del certificado que alojan, serán sometidos a sumario administrativo, tanto el titular que lo cedió como el agente que lo usó en su nombre. La infracción a esta norma será considerada falta grave.

ART. 11. SANCIONES.
Será pasible de sanciones de conformidad con la Ley Orgánica para la Administración de Justicia, quien no cumpla en tiempo y forma las obligaciones precedentes.

ART. 12. POLÍTICAS DE SEGURIDAD:
Se consideran parte integrante del presente Reglamento las Políticas de Seguridad que se adjuntan en calidad de Anexo.

CAPÍTULO II
CONSULTA DE EXPEDIENTES

ART. 13. PRINCIPIO GENERAL.

En todos los casos en que los Códigos Procesales refieren a la disponibilidad del expediente en Secretaría, se entenderá por tal la accesibilidad del mismo en la web.

La notificación tácita de las actuaciones se cumplirá con la disponibilidad de las mismas en el sistema de consultas del expediente electrónico.

Cuando un expediente no pueda accederse por quien está legitimado, éste podrá dejar constancia de tal circunstancia mediante cualquier medio fehaciente de comunicación, incluso correo electrónico dirigido al Secretario. Dicha imposibilidad deberá certificarse por Secretaría de Informática Judicial.

ART. 14. NIVELES DE ACCESO. RESERVADOS. REQUISITOS:

1. La consulta pública de las novedades de cada expediente tramitado en las dependencias del Poder Judicial de San Luis para usuarios externos, está disponible para todas las personas, con diferentes niveles de acceso a la información; a saber:

A.- Acceso restringido al listado de Despacho Diario de expedientes en trámite de cada organismo: Público en General.

B.- Visualización de contenidos de los expedientes en que actúan: Partes del Juicio, sus Apoderados, Representantes legales, Peritos designados, Martilleros, Síndicos, Mediadores, Escribanos y las personas expresamente autorizadas por cualquiera de ellos.

C.- Visualización de contenidos de todos los expedientes públicos: Abogados, incluidos los que se desempeñan en el Poder Judicial, y quienes se autoricen expresamente por Acuerdo específico.

2. En los casos de trámites de carácter reservado, como el que prescribe el art. 197 del CPCC, se dará de alta un incidente con reserva de partes, de manera que la consulta Web quede habilitada sólo para la parte que solicitó la medida.

3. Los interesados en acceder a este servicio de consulta deberán presentarse ante la Secretaría de Informática para solicitar la generación de una casilla de correo electrónico y de una clave de acceso que corresponda a su situación. A ese fin, deberán identificarse y firmar el formulario correspondiente, asumiendo un compromiso de buenas prácticas.

CAPÍTULO III
CONTROL DE GESTIÓN

ART. 15. INFORMES DE AUTOS Y SENTENCIAS.

Los Secretarios deberán efectuar concomitantemente a los actos que ejecuten relativos a pases y recepción de expedientes a resolver, todos los registros necesarios en el sistema informático para conformar los libros de pases a estudio de Autos y Sentencias, a partir de los cuales se generan los informes de autos y sentencias dictados y pendientes en término y fuera de término.

Tales datos se recabarán por Secretaría Administrativa conforme se establezca en el Reglamento de Actuaciones Administrativas a los efectos previstos por la Constitución Provincial y la Ley Orgánica de Administración de Justicia.

ART. 16. INDICES E INDICADORES.

A los fines de extraer información válida y confiable, que cuantifique y cualifique la gestión de cada organismo Jurisdiccional, y que a través de auditorías permita fijar objetivos, los índices, indicadores, estados y actuaciones obligatorias que según los requerimientos funcionales se tornen necesarios, estarán a cargo de una Comisión permanente integrada por Magistrados y Funcionarios de todos los fueros y Circunscripciones designados por el Superior Tribunal. Esta Comisión los definirá, actualizará y revisará de manera permanente.

ART. 17. AUDITORÍAS.

Secretaría Administrativa podrá realizar las auditorías que estime pertinentes, ya sea sobre expedientes físicos o electrónicos, como sobre libros electrónicos.

El área de Auditorías de Secretaría de Informática Judicial, a petición del Superior Tribunal, Secretaria Administrativa, las Excmas. Cámaras de Apelaciones para el ejercicio de las funciones de superintendencia que les asigna la ley Orgánica de Administración de Justicia y Acuerdos reglamentarios, o por orden de la Secretaría de quien depende, es la dependencia encargada de efectuar relevamientos e informes con los datos contenidos en los sistemas informáticos.

TÍTULO II
CONFORMACIÓN DEL EXPEDIENTE ELECTRÓNICO

CAPÍTULO I
INGRESO DE ACTUACIONES

ART. 18. PRINCIPIOS GENERALES

No se recibirán presentaciones de los profesionales abogados en los expedientes, que no sean ingresadas por medios electrónicos.

Para garantizar la integridad y la autenticidad de los escritos que se incorporen por este medio, éstos deberán estar firmados digitalmente, sin excepciones. Asimismo, cuando se adjunte documental digitalizada a la presentación, los archivos correspondientes también deberán estar firmados digitalmente. En todos los casos la firma deberá ser la registrada como profesional matriculado del Colegio profesional que corresponda.

En ningún caso será necesaria la presentación de ejemplares impresos.

En caso de que el sistema de gestión reporte cualquier inconveniente con la firma digital de partes y profesionales, previo a adoptar la medida procesal que corresponda, será responsabilidad de los Funcionarios del Organismo de recepción validarla a través del Instituto de Firma Digital de la Provincia, u otros medios que indique Secretaría de Informática Judicial.

ART. 19. REPRESENTACIÓN CON PATROCINIO LETRADO:

Cuando en el proceso actúen dos profesionales, uno en el carácter de Apoderado y otro ejerciendo el Patrocinio Letrado, deberán firmar digitalmente ambos -al menos- al presentar el primer escrito conjunto; en las presentaciones posteriores bastará la firma del Apoderado y se presumirá que se mantiene el Patrocinio, mientras no se lo reemplace por otro o se aclare que el Apoderado actúa en el doble carácter.

ART. 20. ESCRITOS SIN REPRESENTACIÓN

Para el caso de ingreso de escritos firmados por la parte con patrocinio letrado, el patrocinado deberá firmar con su certificado digital de ciudadano.

Si la parte no contase con firma digital de ciudadano, el Abogado confeccionará el documento, lo imprimirá, lo hará firmar en su presencia por el patrocinado, y subirá al sistema ambas versiones del documento: el original y la imagen digitalizada del papel firmado.

El profesional asume el carácter de depositario judicial de los documentos que ingrese bajo la modalidad señalada precedentemente, con cargo de presentar los originales que haya digitalizado cuando se lo requiera el magistrado competente.

ART. 21. CONTROL DE INGRESOS:

Los Secretarios tienen la obligación de controlar diariamente el ingreso de escritos vía Web por parte de los justiciables, procurando su despacho en término, especialmente cuando contengan pedido de habilitación de día y hora.

Los plazos procesales se contarán a partir del cargo o del envío -art. 34 inc. 3 a) del CPCyC y concordantes- según se trate de escritos o expedientes, por lo que la aceptación en el sistema informático de un documento o de un expediente no incide en dicho cómputo.

ART. 22. CARGO ELECTRÓNICO

Los escritos podrán ser ingresados en cualquier día y hora y se proveerán en horario hábil, salvo lo que se decrete con habilitación.

Ingresado un escrito en el sistema de gestión informática, el cargo electrónico que emite el sistema tendrá plena validez y suplirá al sello de cargo manual.

ART. 23. PLAZO DE GRACIA

Los Sres. Profesionales deberán adoptar las previsiones necesarias para que las presentaciones que pretendan ingresar vía web en el plazo de gracia que prevé el art. 124 del C.P.C. y C., y art. 36 del C.P.L, ingresen dentro del horario del mencionado plazo, a los fines de evitar la extemporaneidad de las mismas, por eventuales contingencias tecnológicas.

ART. 24. PROVIDENCIA DE ESCRITO ELECTRÓNICO

Las providencias deberán individualizar claramente los escritos que se proveen. La visualización mediante la consulta Web del expediente en Internet cumplirá el requisito de copias para traslado.

ART. 25. REUBICACIONES, DESGLOSES Y TESTADOS:

Los escritos externos que hayan sido aceptados erróneamente en un expediente, se reubicarán en el que corresponda, mediante la funcionalidad que brinda el sistema de gestión informática.

Cuando el Juez disponga el desglose de actuaciones internas que hayan sido publicadas para la consulta Web de expedientes, o de actuaciones externas firmadas digitalmente, ello se concretará directamente por el Secretario en el sistema informático una vez firme el decreto que ordena el desglose.

Cuando un juez mande testar una frase injuriosa o escrita en términos indecorosos u ofensivos, si la frase en cuestión estuviera contenida en un documento electrónico firmado digitalmente, el Juez podrá ordenar su desglose y reemplazo por copia fiel en la que se ejecute el testado por parte del Actuario, quien firmará digitalmente el documento resultante.

ART. 26. ACTUACIONES DOCUMENTADAS EN SOPORTE PAPEL:

Las actuaciones documentadas en soporte papel existentes en expedientes mixtos a la fecha del comienzo de la despapelización en cada Organismo, se conservarán en Secretaría, a disposición de los interesados para su compulsa, hasta que la causa esté en condiciones de ser archivada.

ART. 27. PRESENTACIÓN DEL ESCRITO INICIAL:

a) Para el inicio de nuevas causas los profesionales deberán comparecer ante Mesa General Única o al Juzgado, en los casos en que no corresponda la intervención de aquélla; a fin de solicitar el alta del expediente respectivo, en el cual ingresará posteriormente por sí y por los medios electrónicos habituales la demanda, denuncia o presentación y la documental adjunta, si la hubiere. El plazo a los efectos procesales se computará a partir del cargo electrónico de esta presentación.

El alta de expediente también podrá ser solicitada por medio de correo electrónico dirigido a la Mesa General Única o al Juzgado, en los casos en que no corresponda la intervención de aquélla. En el asunto deberá indicarse claramente que se solicita el alta de nueva causa, y deberá adjuntarse un documento firmado digitalmente en donde consten todos los datos del formulario pertinente que se encuentra disponible en la página web del Poder Judicial.

Los ingresos que efectúen los Sres. Síndicos de las insinuaciones de créditos, se realizarán directamente ante el Juzgado correspondiente, siguiendo el procedimiento descripto.

b) Para el traslado de esta presentación, el Abogado confeccionará la cédula papel que se diligenciará con las copias que deberá adjuntarle, salvo en los fueros en los que corresponde el impulso de oficio.

Diligenciada la cédula, será digitalizada y devuelta al presentante, o destruida luego de transcurrido el plazo de un mes desde su incorporación en el expediente judicial electrónico.

ART. 28. ESCRITO DE CONTESTACIÓN

En el primer escrito de la demandada o citada de conformidad con el artículo precedente, los profesionales deberán:

1- Si se trata de expedientes públicos, ingresar electrónicamente por el sistema de gestión on line la totalidad de los escritos y documental digitalizada.

2- Si se trata de expedientes con reserva de partes y no se ha levantado la restricción, el representante o patrocinante del demandado deberá comparecer ante el Juzgado a fin de solicitar su vinculación personal en el sistema informático para proceder luego a ingresar la contestación por los medios electrónicos habituales.

Tal solicitud también podrá efectuarse vía correo electrónico al Juzgado correspondiente. En el asunto deberá indicarse claramente que se solicita la vinculación en un expediente para contestar traslado, aclarando los datos de nombre, domicilio y documento de su representado o patrocinado.

Si no se hubiere posibilitado el acceso al expediente en tiempo oportuno, la contestación podrá ingresarse por correo electrónico dirigido al Juzgado, adjuntando los documentos que cupiere, firmados digitalmente. Certificada la imposibilidad por Secretaría de Informática, el juez evaluará la prórroga del plazo.

La situación podrá ser denunciada ante Secretaría de Informática Judicial, quien con el informe pertinente elevará las actuaciones a la Oficina de Sumarios Administrativos, para la tramitación pertinente.

ART. 29. PRUEBA DOCUMENTAL

a) En todos los casos, luego de ingresarse la digitalización de documental, los originales deberán presentarse en el plazo de un día hábil, a contar desde el cargo electrónico de la presentación, en la Secretaría del Juzgado. El Secretario, comprobada la correspondencia con los documentos electrónicos agregados al expediente, dejará constancia en el expediente de tal circunstancia y reservará provisoriamente los originales.

Posteriormente, una vez vencido el traslado a la contraria o resuelta la eventual impugnación, se devolverán los documentos, debidamente visados por el Actuario, al presentante. Éste deberá retirarlos y recibirlos en carácter de Depositario

Judicial con cargo de presentarlos nuevamente, en caso de que lo requiera el Magistrado competente, o deba efectuarse pericia o reconocimiento. El incumplimiento de esa carga dará lugar a las responsabilidades civiles y penales de Ley.
La demora en la presentación de los originales configura una conducta que habilita a los Sres. Magistrados para el uso de las facultades ordenatorias que establece el art. 36 inc. 1 del Código de Procedimientos Civil y Comercial, como así de la potestad correctiva que regulan los arts. 30 y 31 de la Ley Orgánica Nº IV-0086-2004.-

b) Cuando las características de los documentos impidiesen su digitalización, podrán presentarse directamente ante la Secretaría correspondiente, quien informará al Magistrado en caso de que la imposibilidad sea absoluta, para la adopción de las medidas de resguardo pertinentes.

ART. 30. PLAZO DEL PROCEDIMIENTO. OPCIÓN DEL INTERESADO:
Cuando deba efectuarse la digitalización de actuaciones y documental presentada por terceros, ésta se efectuará dentro de las veinticuatro horas de la recepción, cuando el total de documentos a escanear no exceda de cincuenta fojas. Pasado dicho margen, quedará a criterio del Secretario o responsable de la Oficina de Digitalización, en su caso, el plazo en que se efectuará el proceso. En todos los casos queda a voluntad del interesado traer los documentos ya digitalizados en un soporte electrónico, para ser cotejados y firmados digitalmente por el Actuario del tribunal donde tramite la causa.

ART. 31. AUDIENCIAS.
1. Cuando una audiencia se documente en archivos multimedia será firmada digitalmente por el Secretario y por las partes que posean certificado de firma digital en su caso. Tal documento multimedia deberá incorporarse al sistema de gestión informática como una actuación más del expediente electrónico.

Idéntico concepto se aplica a las audiencias orales de las causas penales en trámite ante las Excmas. Cámaras del fuero, quedando reemplazada el acta por el archivo digital de videograbación.
Queda autorizado el uso de archivos digitales de video grabación firmados digitalmente por la Sra. Secretaria del Jurado de Enjuiciamiento en la realización de las Audiencias Orales que tramiten ante ese Tribunal. El archivo digital, con el requisito de ley mencionado precedentemente, reemplaza en forma eficiente y válida el Acta de Audiencia de que prevé el art. 41 inc. 7 de la Ley de Jury N° VI-0478-2005.

2. En los demás casos, las actas de las audiencias se confeccionarán en sistema informático, con la aclaración del Secretario en pie de página de quienes firman en su presencia la copia impresa y suscribirá digitalmente el documento. Cuando el juez hubiera presidido la audiencia y cuando algún compareciente tuviera certificado de firma digital, también firmarán el documento electrónico.
En su caso, las actuaciones con firmas manuscritas se resguardarán en biblioratos hasta la finalización de la causa, sin agregarse al expediente electrónico.-

CAPÍTULO II
MINISTERIOS PÚBLICOS

ART. 32. PRINCIPIO GENERAL:
En los casos en que los Ministerios Públicos de la Defensa y de la Acusación inicien causas ante los Juzgados de Primera Instancia, esa iniciación deberá hacerse dando el alta de la nueva causa en el sistema informático, vinculando debidamente las partes, incluyendo la digitalización de documentos que cupiere adjuntar, y efectuando el pase consecuente al organismo de destino, o solicitando sorteo de Juzgado ante Mesa General Única, según corresponda.

ART. 33. ESCRITOS POSTERIORES

Los escritos posteriores podrán ingresarse como actuación del sistema informático interno o como escrito electrónico externo vía web, según la disponibilidad del expediente.
Cuando dichos Funcionarios deban tomar participación en un expediente en trámite, la primera notificación a los mismos se efectuará, en todos los casos, con el pase en vista del expediente electrónico, previa vinculación del Organismo.

CAPÍTULO III
MESA GENERAL ÚNICA

ART. 34. COMPETENCIAS:

1. La Mesa General Única, que depende de Secretaría Judicial, será la vía de ingreso y asignación por sorteo compensatorio y aleatorio de todas las causas que deban tramitar ante los juzgados de primera instancia civil, comercial, minas, laboral, familia civil, y paz letrado. También recibirá los Oficios y Exhortos Ley 22.172 a cuyo fin deberá controlar diariamente la casilla de correo electrónico oficioley@justiciasanluis.gov.ar.
En ningún caso recibirá expedientes físicos remitidos desde los organismos que reclamen su reasignación.
2. Todos los incidentes serán dados de alta en el sistema por los Juzgados en donde se inicien.
3. Para la asignación de causas a los Juzgados de Familia, su competencia está restringida exclusivamente a causas del fuero Civil. Quedan expresamente excluidas de ésta intervención las causas penales, de violencia, tutelares, comunica situación, situaciones de riesgo o vulnerabilidad psicosocial, las que se ingresarán en forma directa al Juzgado de Familia que por turno o conexidad corresponda. Cuando se trate de presentaciones de esta naturaleza y sin firma de letrado, las mismas deberán ser digitalizadas por el Secretario competente.
4. Todos los correos electrónicos que reciba en el marco del presente Reglamento, deberán ser contestados en el término de un día desde la recepción.

5. La Mesa General Única tendrá la función de digitalización de documentos que deban incorporarse a las causas judiciales, a solicitud de los funcionarios responsables de cada organismo, cuando el volumen lo justifique. El responsable de Mesa General Única, será el fedatario de la documentación que digitalice.

ART. 35. FORMULARIO DE INGRESO DE CAUSAS:

Para solicitar el alta de expedientes, los litigantes deberán presentar -llenado de conformidad a las instrucciones que contiene y debidamente firmado por el letrado interviniente- un ejemplar del "Formulario para ingreso de Causas", que estará disponible para su impresión por los interesados en el sitio Web del Poder Judicial. El mismo tiene carácter de declaración jurada.

ART. 36. AMPAROS:

En los casos de Amparos, en cumplimiento de la Ley IV-0090-2004, la Mesa General Única asignará manualmente el Juzgado que indique el profesional presentante.

ART. 37. ASIGNACIÓN DE CÁMARA:

La Mesa General Única asignará la Cámara de Apelaciones que deberá entender en un expediente, cuando ocurra la primera elevación a la alzada desde los Juzgados de primera instancia.

Las elevaciones subsiguientes, en todos los casos, se harán en forma directa y sin necesidad de informe alguno, por el juzgado donde tramite la causa, tomando del sistema la información de cuál es la Cámara que ha entendido con anterioridad. Este control será único y suficiente para habilitar el trámite.

Los Juzgados de Instrucción en lo Penal, Correccional y Contravencional, de la Primera y Segunda Circunscripción Judicial, al elevar las causas para juicio oral, si hubiera tenido anterior intervención una Excma. Cámara de Apelaciones en lo Penal, Correccional y Contravencional con motivo de recursos de apelaciones, deberán hacerlo directamente a la otra Cámara.

En todos los casos compensará la carga de causas de acuerdo con los parámetros que establezca el Superior Tribunal por vía de Acordada.

ART. 38. RECURSO DE QUEJA:

Los recursos de queja, cuando corresponda sortear Cámara, ingresarán directamente por MGU debiendo el profesional seguir el procedimiento previsto para el ingreso de nuevas causas.

Las quejas que deban presentarse ante el Superior Tribunal o la Cámara de Apelaciones de la Tercera Circunscripción sin previo sorteo, se ingresarán por vía electrónica, previa solicitud al Organismo, presencialmente o por correo electrónico, del alta del expediente en cuestión. Si se optase por correo electrónico deberán cumplirse los recaudos indicados para los escritos iniciales en los artículos precedentes.

ART. 39. INGRESO MASIVO DE CAUSAS:

La Mesa General Única sorteará expedientes ingresándolos en forma masiva a través del sistema informático, a partir de la presentación en soporte electrónico de una planilla donde se individualicen las nuevas causas.

Los presentantes no deberán incluir en una misma planilla expedientes que deban ingresarse manualmente en un determinado juzgado y expedientes que deban ser sorteados. De darse el caso, deberán presentarse en planillas separadas según estas categorías.

ART. 40. CAMBIOS DE RADICACIÓN ORIGINARIA:

En los casos de cambio de radicación de un expediente, el Juzgado que siga en orden de turno se asignará por sorteo incluyendo –en caso de agotarse un fuero- los fueros restantes, en el siguiente orden: civil, laboral, penal, luego al Juzgado de Paz Letrado y, finalmente, sorteo entre los Juzgados de Familia.

Cuando se produzca una excusación, recusación, inhibición, apartamiento, nulidad dictada por las Cámaras, o cualquier causa que importe cambio de radicación, el

juzgado deberá retornar el expediente por sistema a MGU para su nueva radicación.

CAPÍTULO IV
OTROS ORGANISMOS

ART. 41. ORGANISMOS AUXILIARES:
Todos los organismos auxiliares que dependen del Superior Tribunal tramitarán en el sistema informático de gestión judicial todos los procedimientos en que intervengan.
Los requerimientos que se efectúen a los Centros de Mediación, Registro Único de Adoptantes, Oficina de Secuestros, Cuerpo Profesional Forense, Órgano de Contralor de Tasas, Oficina de Sumarios Administrativos, Oficina de denuncias, y otros, deberán efectuarse por las vías de comunicación disponibles en el sistema de gestión, siguiendo las reglamentaciones y las indicaciones de Secretaría de Informática Judicial.

ART. 42. REGISTRO DE JUICIOS UNIVERSALES:
Registro Inicial:
I.- Al solicitarse ante la Mesa General Única el alta de juicios testamentarios, sucesorios ab intestato, y protocolización de testamentos, ésta procederá al alta solicitada y a generar un expediente relacionado, que remitirá al Registro de Juicios Universales.

II.- Recibido el expediente relacionado por el Registro de Juicios Universales, éste hará constar el inicio de la causa principal mediante una actuación firmada digitalmente, siendo en consecuencia inoficiosa la comunicación del Secretario del Juzgado, respecto del inicio de éstos juicios, que enuncia el art. 116 de la Ley Orgánica de Administración de Justicia. El número del expediente relacionado “RJU” será el número de inscripción en el Registro de Juicios Universales.

III.- Seguidamente, consultará sobre la existencia de otros procesos universales, tanto en la base digitalizada de datos anteriores, como en los registros del sistema y emitirá informe al Juzgado sobre el resultado de la búsqueda, dentro de los diez días de recibido el expediente relacionado remitido por Mesa General Única.

Comunicaciones posteriores:

IV.- La inscripción de las actuaciones sobre declaratorias de herederos dictadas en otras jurisdicciones, resoluciones de aperturas de concursos, homologación de concordatos, liquidaciones sin declaración de quiebra, calificación en las quiebras, y rehabilitación en quiebras o concursos, como también la rectificación de los nombres del causante o concursado, será efectuada previa comunicación del Secretario del Juzgado interviniente, mediante Oficio Relacionado, al Registro de Juicios Universales.

V.- Efectuada la toma de razón en los expedientes relacionados, éste organismo devolverá el Oficio Relacionado dentro de los diez (10) días con una actuación firmada digitalmente por el encargado del Registro de Juicios Universales, donde informará sobre la inscripción y demás datos, debiendo corroborar con esos datos, la información sobre la existencia de cualquier juicio similar con respecto al mismo causante.

VI.- Los pedidos de informes posteriores al Registro de Juicios Universales por parte de Organismos del Poder Judicial, se realizará por medio de Oficio Relacionado. Los que soliciten los particulares o profesionales, mediante nota y previo pago de la tasa pertinente, se generarán en los expedientes relacionados.

TÍTULO III
TRAMITACIÓN DEL EXPEDIENTE

CAPÍTULO I
NORMAS GENERALES

ART. 43. RECEPCIÓN DEL EXPEDIENTE. BANDEJA DE PENDIENTES:

Cuando un expediente ingresa en un organismo por remisión desde otro, es obligación del receptor dar recibo en el sistema informático, dentro de las 24 hs. desde que se efectuó el pase.
En caso de que el pase sea erróneo, el organismo destinatario deberá aceptar el expediente y devolverlo al emisor, haciendo constar tal circunstancia en las observaciones del pase.
Será considerada falta grave la omisión de las acciones precedentes.

ART. 44. EXPEDIENTES COMO PRUEBA:
Cuando las constancias de un expediente deban cotejarse en el trámite de otro, si se encuentran digitalizadas en el sistema de gestión informática, se solicitará el pase externo para visualización de las mismas, que permite su evaluación a través de los medios electrónicos de consulta en línea, sin remisión.

ART. 45. EXPEDIENTES HISTÓRICOS Y MIXTOS:
Para el caso de generarse actuaciones en expedientes que obren en soporte papel y no se registren en el sistema informático, deberá solicitarse a la Mesa General Única el alta de los mismos en el sistema radicándolos en forma manual en el juzgado de origen.
Para el caso de cambios de radicación de expedientes históricos sin ningún registro en el sistema informático, el Secretario del Juzgado que se desprende del expediente deberá solicitar a la Mesa General Única el alta en el sistema del expediente y el sorteo para la nueva asignación. Esta solicitud podrá efectuarse por correo electrónico.
En el caso de expedientes mixtos, que contengan actuaciones en el sistema y otras sólo en soporte papel, recibido el pase electrónico sin acompañar estas últimas, al finalizar la jornada laboral se devolverá al emisor, haciendo constar tal circunstancia en las observaciones del pase.

ART. 46. ARCHIVO DE CAUSAS QUE NO SE ENCUENTREN REGISTRADAS EN LOS SISTEMAS INFORMÁTICOS:

Cuando deban remitirse al archivo para su destrucción causas -y documentación- concluidas o paralizadas en las dependencias o bauleras y estas no se encuentren asociadas a ninguna registración electrónica, no será necesaria la previa carga de las mismas en el Sistema de Gestión Informática.

ART. 47. RESPONSABILIDAD COMPLEMENTARIA DE LOS JUZGADOS:
Toda modificación de carátula o de cualquier dato de la carga inicial que hubiere efectuado MGU, que dispongan los Jueces, será efectuada por el Juzgado de radicación del expediente. Asimismo el juzgado subsanará cualquier error u omisión en la carga inicial, especialmente en los campos de tasas de justicia y los datos del demandado y su representante, que habitualmente no son aportados al momento del ingreso del juicio nuevo en MGU.

ART. 48. RESPONSABILIDAD DE LOS PROFESIONALES.
El plazo máximo para la presentación de la demanda luego del alta por Mesa General Única, es de un día. Si se hubiera solicitado el alta por correo electrónico, dicho plazo se contará desde la recepción de la respuesta.
La demora en concluir el trámite de presentación de la causa excediendo del plazo indicado, configura una conducta sancionable que habilita a los Sres. Magistrados para el uso de las facultades ordenatorias que establece el art. 36 inc. 1 del Código de Procedimientos Civil y Comercial, como así de la potestad correctiva que regulan los arts. 30 y 31 de la Ley Orgánica Nº IV-0086-2004.
Las sanciones que apliquen los Jueces por los incumplimientos que refiere este Acuerdo, serán pasibles de Recurso de Reconsideración con Apelación en Subsidio ante este Superior Tribunal de Justicia.

CAPÍTULO II
DESPACHO DIARIO

ART. 49. DESPACHO COMÚN:

Es obligación de los Sres. Jueces y Secretarios asegurar la publicación de los despachos diarios de expedientes hasta la hora siete con treinta minutos de cada día hábil de oficina. Para ello los decretos y demás actuaciones que deban publicarse, deberán firmarse digitalmente en el sistema hasta la hora veintidós del día previo. Pasada esa hora, las actuaciones que se firmen no publicarán en el despacho del día inmediato posterior sino al siguiente hábil.

ART. 50. DESPACHO CON HABILITACIÓN:
Los despachos salidos con habilitación de día y hora deberán corresponder a escritos presentados con una antelación máxima de veinticuatro horas al proveído a publicarse. Cuando la diferencia horaria entre pedido y decreto supere dicho límite, deberá incluirse en el despacho común que corresponda.

ART. 51. PUBLICACIÓN:
Se publicarán en el sitio web del Poder Judicial los despachos diarios. Los proveídos con habilitación de día y hora se publicarán a partir de su firma por el Magistrado, aún en horario inhábil; los demás se publicarán en el despacho diario común, al día siguiente.

CAPÍTULO III
DESIGNACIÓN DE AUXILIARES INSCRIPTOS

ART. 52. SORTEO POR SISTEMA INFORMÁTICO:
El sorteo de los Peritos, Escribanos y Martilleros inscriptos en la Secretaría Administrativa del Superior Tribunal de Justicia, deberá realizarse a través del Sistema de Gestión Informática, en base a la nómina de profesionales habilitados en la especialidad correspondiente y que son cargados en el sistema.
Los que resulten sorteados no serán nuevamente incluidos hasta agotar la lista.
Igual procedimiento se seguirá para el sorteo de los Síndicos inscriptos ante las Cámaras de Apelaciones en lo Civil, Comercial, Minas y Laboral.

CAPÍTULO IV
COMUNICACIONES ELECTRÓNICAS

ART. 53. OFICIOS DILIGENCIADOS POR LOS ORGANISMOS JUDICIALES

1. Cuando los Oficios estén dirigidos a organismos de la estructura del Poder Ejecutivo de la Provincia y a cualquier otra entidad o sujeto público o privado que cuente con Firma Digital reconocida por Convenio Específico por este Poder Judicial de la Provincia, serán diligenciados en el sistema informático por los Secretarios conforme la tecnología disponible en cada caso.

2. La confección del Oficio dependerá de la atribución de la carga que determinen los Códigos de Procedimiento; si recayera en los profesionales, éstos deberán presentar un escrito electrónico adjuntando el documento del oficio en formato editable para control y posterior tramitación.

3. Cuando la carga procesal esté atribuida a los organismos judiciales, y deban diligenciarse necesariamente en soporte papel, se confeccionarán en el sistema de gestión informático y sólo se imprimirán en dos ejemplares, uno para ser entregado a la entidad oficiada, y el otro para ser digitalizado y agregado al expediente como constancia del diligenciamiento.-

4. Los oficios dirigidos al Banco Oficial en todos los casos y fueros, estará a cargo de los Sres. Secretarios.

El envío de los oficios deberá concretarse dentro de los cinco días hábiles de ocurrida la publicación de la resolución que los ordena. La contestación deberá obrar como actuación del expediente electrónico.

Los pedidos de apertura de cuenta judicial podrán ser solicitados por el abogado desde su casilla de correo institucional, adjuntando la orden judicial que le da sustento.

5. Las comunicaciones y/o notificaciones dirigidas al Colegio de Escribanos de la Provincia de San Luis que se emitan en virtud de las previsiones de la Ley Nº XIV-0360-2004 (5721 “R”) y toda otra que se disponga en el ámbito de este Poder

Judicial, se efectuarán a la casilla de correo electrónico en el dominio escribanossl@giajsanluis.gov.ar.

ART. 54. OFICIOS DILIGENCIADOS POR LOS PROFESIONALES:

1. Principio General:

Cuando los Códigos de Procedimiento ponen la responsabilidad de la tramitación de los Oficios en cabeza del profesional que ofreció la medida, será necesaria la presentación del documento en soporte electrónico.

2. Trámite papel firmado por el profesional:

En los casos del art. 400 del CPCC, los profesionales Abogados que cuenten con su certificado de firma digital podrán ingresar el Oficio directamente al expediente con la respuesta del oficiado, mediante el procedimiento de ingreso de escritos vía web.

3. Trámite papel firmado por Actuario:

En el trámite de Oficios que no sean los previstos en el art. 400 del CPCC y que deban diligenciarse en papel, el Abogado deberá presentar un escrito electrónico adjuntando el documento del oficio para control en formato editable. Efectuado el mismo, se incluirá el documento en el sistema de gestión, firmado por el Secretario. El Abogado, con el texto publicado ya impreso, se presentará en Secretaría para que, en esa oportunidad, el Secretario firme el ejemplar en soporte papel que se diligenciará.

ART. 55. OFICIOS Y EXHORTOS LEY 22.172

A los fines de las comunicaciones interjurisdiccionales se seguirá el procedimiento establecido en el Convenio de Comunicación Electrónica Interjurisdiccional y su Protocolo Técnico, acordados en el seno de la Junta Federal de Cortes y Superiores Tribunales de las Provincias Argentinas y Ciudad Autónoma de Buenos Aires.

La recepción estará a cargo de Mesa General Única de la Primera Circunscripción quien deberá proceder a los sorteos o remisiones pertinentes dentro de la Primera Circunscripción, o remisión a dichos efectos a Mesa General Única de la Segunda o a los Organismos pertinentes de la Tercera Circunscripción Judicial, y posteriormente comunicar al remitente, por el mismo medio, qué organismo será el responsable de la tramitación, informando como mínimo nombre de funcionario, correo electrónico y teléfonos.-

El envío de Oficios y Exhortos electrónicos se efectuará por correo a las direcciones publicadas en el sitio web de cada Poder Judicial.

ART. 56. SUMARIOS POLICIALES:

Los Sumarios de Prevención que generan las distintas Comisarías de la Provincia deberán comunicarse por sistema informático a las dependencias pertinentes de este Poder Judicial.

Cuando exista alguna imposibilidad técnica para la comunicación entre sistemas, la remisión se efectuará por correo electrónico emitido desde y hacia la casilla institucional. Las oficinas judiciales deberán incorporar al sistema de gestión los archivos remitidos por la Policía, para dar urgente inicio al trámite correspondiente.

Las comunicaciones que se efectúen durante la tramitación del sumario, se canalizarán por interacción electrónica entre la Policía y el Juzgado interviniente. Cuando las solicitudes y decisiones se adelanten telefónicamente, se dejará constancia actuarial en el expediente.

ART. 57. COMUNICACIONES ADMINISTRATIVAS INTERNAS:

Las comunicaciones internas del Poder Judicial, cuando el contenido a comunicar no resulte del sistema de gestión informática, se efectuarán desde y hacia las casillas de correo electrónico institucionales pertinentes, adjuntando el archivo que contenga el documento, firmado digitalmente. La misma se considerará cumplida con la sola recepción en la casilla del destinatario, debiendo a esos efectos enviarse el correo con confirmación de entrega.

ART. 58. COMUNICACIONES EN EXPEDIENTES JUDICIALES:
Las comunicaciones jurisdiccionales entre todos los organismos de la estructura del Poder Judicial deberán efectuarse a través del sistema de gestión informático, sea mediante un pase del expediente, creando un expediente relacionado, o emitiendo un oficio electrónico.

ART. 59. MANDAMIENTOS:
Los Mandamientos serán confeccionados por los Secretarios en el sistema informático y remitidos por esta vía, sin copia papel, a la oficina respectiva que deberá diligenciarlo, entregando copia impresa en el momento de la diligencia y devolviendo al tribunal de origen el Mandamiento debidamente informado por sistema y firmado digitalmente por el Oficial de Justicia interviniente.
La Oficina de Mandamientos y Notificaciones deberá proceder a la devolución a los Juzgados o Tribunales que correspondan, de todas las copias en soporte papel de los Mandamientos diligenciados, con documentación original –planos, escrituras, etc.-, existentes en dicha dependencia y que ya se hayan remitido sólo por sistema informático.

CAPÍTULO V
NOTIFICACIONES POR CÉDULA PAPEL

ART. 60. ACLARACIONES DE PROCEDIMIENTO:
Las llamadas notificaciones en Estrados del Juzgado importan la remisión legal a la notificación automática de martes y viernes y no deben generar ningún tipo de impresión de cédula alguna, ni para diligenciar, ni para exponer en el expediente, ni en ningún espacio físico de Tribunales.
La notificación por cédula impresa requiere solamente de dos ejemplares del documento, uno que se deja al notificado y otro que es devuelto al juzgado por el Oficial Notificador con la constancia de la diligencia. Este ejemplar se digitalizará y agregará al expediente dentro del plazo de veinticuatro horas, y se destruirá a los treinta días.

Se enviarán en soporte papel -a través de la Oficina de Notificaciones- las que se ordenen previo a la constitución de domicilio legal electrónico del destinatario, las dirigidas a domicilio denunciado y real y las que –destinadas a domicilios constituidos- deban adjuntar copias de documentos que no puedan digitalizarse en el sistema de gestión en uso interno del Poder Judicial.

ART. 61. CONTROL DE DOMICILIOS CONSTITUIDOS:
Para las notificaciones que no admiten cédula electrónica, a los fines de la confección por sistema de la planilla de cédulas que deberán diligenciarse por los notificadores, es obligatoria la carga del campo “domicilio constituido”; para lo cual los Secretarios deberán controlar los cambios de domicilio que ocurran en cada expediente a fin de mantener los datos actualizados en el sistema.

ART. 62. TRÁMITE DEL LOTE DE NOTIFICACIONES:
Los Sres. Secretarios deberán asegurar el envío diario del número de lote de las notificaciones por cédula papel generadas, como así la remisión de los respectivos instrumentos a la Oficina de Notificaciones, antes de la hora ocho. Deberán además disponer el retiro, en esa oportunidad, de las cédulas ya diligenciadas que se encuentren disponibles en la oficina, bajo su responsabilidad.

CAPÍTULO VI
NOTIFICACIÓN ELECTRÓNICA

ART. 63. DOMINIOS AUTORIZADOS:
La implementación del sistema de notificación por medio de la cédula que genera el sistema de gestión informática de administración de Justicia, se basa en la utilización del correo electrónico de los dominios justiciasanluis.gov.ar y giajsanluis.gov.ar, exclusivamente.

ART. 64. LA CÉDULA: CONTENIDO. FIRMA. ENVÍO. EFECTOS:

La cédula de notificación electrónica deberá respetar en cuanto a su formato y contenido las disposiciones vigentes en los Códigos Procesales de la Provincia de San Luis, propiedades que permitan al destinatario efectuar el control de la firma digital de la cédula. El envío de la notificación deberá efectivizarse una vez firmada digitalmente y publicada la providencia que la ordena. A los fines del cómputo de los plazos de las notificaciones por cédula, que indican los Códigos de Procedimientos, el día y hora del envío a la casilla del destinatario que informa el servidor marcará el inicio del plazo procesal que corresponda.
El Secretario deberá revisar la casilla institucional del Juzgado para constatar los eventuales casos de rechazo de notificaciones.

ART. 65. MODALIDADES DE LA NOTIFICACIÓN. PLAZO DE ENVÍO:
La obligación de notificar por cédula, en todos los casos y fueros, salvo las excepciones expresamente dispuestas, estará a cargo de los Sres. Secretarios. Se enviarán por medios electrónicos todas las que deban destinarse a domicilios constituidos. El envío de las cédulas deberá concretarse dentro de los cinco días hábiles de ocurrida la publicación de la resolución que notifican.

ART. 66. NOTIFICACIONES POR POLICÍA DE LA PROVINCIA:
Las notificaciones que se concretan a través de la Policía de la Provincia, se solicitarán por las dependencias judiciales competentes por medios electrónicos.

ART. 67. CONSTITUCIÓN DE DOMICILIO. OBLIGATORIEDAD:
El profesional que litigue por propio derecho o por representación y los auxiliares designados judicialmente, deberán constituir en cada expediente en que intervengan su domicilio legal electrónico registrado en la base de datos del sistema. Su constitución deberá concretarse en la oportunidad del art. 40 del CPCC. Los que no cumplan con la obligación de constituir domicilio electrónico en el expediente, quedarán notificados de las sucesivas providencias en los Estrados del Juzgado o Tribunal, en los términos y alcances del art. 41 del CPCC, sin necesidad de intimación previa ni de providencia que así lo indique.

La obligación de constituir domicilio legal electrónico alcanza a los Síndicos designados en los expedientes concursales. Se tendrá por suficientemente cumplida con la constitución del mismo en el expediente principal y operará en todos los relacionados.

ART. 68. OBTENCIÓN DEL DOMICILIO ELECTRÓNICO:
Para la constitución del domicilio electrónico, el profesional que aún no haya tramitado su casilla de correo y clave de acceso a la consulta Web de expedientes, deberá obtener, con carácter obligatorio, la generación de una casilla de correo ante la Secretaría de Informática, bajo apercibimiento de Ley.

ART. 69. UNIFICACIÓN DEL DOMICILIO:
Sin perjuicio de que en los casos que a una misma parte la representen más de un profesional, podrán emitirse cédulas electrónicas a todos los que estén relacionados en el expediente, considerando a estas otras notificaciones como de cortesía.

ART. 70. CONTROL DEL DOMICILIO CONSTITUÍDO:
El domicilio electrónico constituido en el expediente deberá ser controlado por Secretaría. Cuando éste no coincida con el domicilio registrado en la base de datos, se deberá verificar el domicilio correcto con la Secretaría de Informática y – en caso que exista un error en su individualización por el profesional - el Tribunal deberá intimar su rectificación en un plazo de cinco días, vencido el cual el único domicilio electrónico válido, al cual se remitirán la notificaciones, será el registrado en la base de datos correspondiente. Si el domicilio constituido es el correcto no requerirá ser proveído y surtirá efecto desde su constitución.

ART. 71. NOTIFICACIÓN POR ABOGADOS. MODALIDAD:
Quedan exceptuadas de la notificación por Secretaria las cédulas dirigidas a los testigos ofrecidos por las partes, los que serán citados por los profesionales abogados interesados presentando las cédulas en soporte papel.

Los representantes de las partes que decidan hacer uso de la facultad del art. 136 del CPCC, al emitir una notificación electrónica la dirigirán directamente a sus destinatarios, sin previo control de la dependencia judicial. A ese fin, el profesional notificará a la contraparte con un correo electrónico que contenga como texto (cuerpo de mail) el documento del art. 137 del CPCC y lo enviará con la opción de confirmación de entrega al destinatario (no la de lectura), que ofrece el correo institucional.

Inmediatamente de cumplir la diligencia deberá ingresar en el sistema, y agregar al expediente que corresponda sólo la cédula de notificación y el correo que recibe del Administrador del sistema de confirmación de entrega, sin necesidad de escrito aclaratorio.

ART. 72. HORARIO DE NOTIFICACIONES:

El proceso de envío de notificaciones se cerrará a las diecinueve horas (19 hs) de cada día hábil, para posibilitar a los profesionales el control diario de las notificaciones recibidas. Quedan exceptuadas de esta limitación las notificaciones del fuero penal y administrativas y las de los restantes fueros que se ordenen con habilitación de día y hora.

ART. 73. SERVICIO PENITENCIARIO. INTERNOS:

Los alojados en el Servicio Penitenciario obtendrán su domicilio electrónico a partir de la orden de internación, a cuyo fin los Jueces del Fuero Penal deberán comunicar por Oficio a la Secretaría de Informática dicha situación, detallando los datos personales del interno. Generado el domicilio electrónico correspondiente, la Secretaría de Informática lo comunicará a la autoridad judicial de la cual dependa el interno y a la Jefatura del Servicio Penitenciario, a sus efectos. Quedan exceptuados del sistema de notificación electrónica los internos analfabetos, para garantizar el resguardo de sus derechos.

ART. 74. SERVICIO PENITENCIARIO. COPIAS:

Las cédulas electrónicas enviadas a los internos del Servicio Penitenciario se deberán enviar con copia al Jefe del Servicio Penitenciario y al Procurador Penitenciario, a cuyo fin se generarán por Secretaría de Informática los domicilios electrónicos correspondientes a dichas funciones.
El Superior Tribunal habilitará un Libro, foliado y rubricado por la Secretaría Judicial, que será entregado a la Jefatura del Servicio Penitenciario a los fines del art. 42 Bis, Ley Prov. VI-0689-2009.

TÍTULO IV
ACTIVIDAD ADMINISTRATIVA

ART. 75. CONSTITUCIÓN COMO AUTORIDAD DE REGISTRO REMOTA:
El Superior Tribunal de Justicia de la Provincia de San Luis, es la Autoridad de Registro Remota de la Autoridad Certificante Provincial, que habilita la obtención de los certificados de Firma Digital de todos los miembros de su estructura orgánica y de los peritos inscriptos y mediadores.
La conducción de la Autoridad de Registro es ejercida por la Dirección de Recursos Humanos.

ART. 76. - SECRETARÍA DE INFORMÁTICA JUDICIAL.
Secretaría de Informática Judicial no recibirá ni responderá comunicaciones impresas de ningún organismo judicial. Todos los pedidos deberán canalizarse por el sistema de gestión, mediante Oficios o pases, y serán respondidos por igual vía.
Para el caso de comunicaciones emanadas de organismos de la estructura administrativa del Poder Judicial que no tengan disponible el sistema de gestión informática, las mismas se efectuarán por correo electrónico, adjuntando el archivo en el que conste el pedido; la eventual respuesta, si cupiere, se enviará como respuesta por igual procedimiento. Todas las comunicaciones deberán ser firmadas digitalmente.
Los trámites internos de la Secretaría se documentarán en expedientes electrónicos.

ART. 77. FACULTADES DE SECRETARÍA DE INFORMÁTICA JUDICIAL

En el ámbito de las atribuciones que le son propias, esta Secretaría podrá emitir, previa autorización del Presidente del Superior Tribunal o Ministro responsable del área, Resoluciones y Memorandums que serán de cumplimiento obligatorio.

ART. 78. DIRECCIÓN CONTABLE. RENDICIONES DE CUENTAS.

La Dirección Contable deberá trabajar con el sistema informático todas las actuaciones y constancias destinadas a conformar los expedientes de rendición de cuentas.

Secretaría de Informática habilitará la consulta de expedientes, en la dependencia correspondiente, al personal autorizado del Honorable Tribunal de Cuentas de la Provincia, quien deberá dejar constancia en los expedientes auditados del resultado de la auditoría.

ANEXO

POLÍTICA DE SEGURIDAD INFORMATICA

DEL PODER JUDICIAL DE SAN LUIS

Introducción

La base para que cualquier organización pueda operar de una forma confiable, ordenada y consciente en materia de Seguridad Informática comienza con la valoración de los riesgos, definición de políticas, estándares, procedimientos de trabajo y mecanismos que permitan medir, auditar, proteger, actuar y mejorar los servicios informáticos en base a la retroalimentación e interacción continua de todos quienes la integran.-

Siendo que la Seguridad Informática es una función en la que se deben evaluar y administrar los riesgos, cubriendo las necesidades del Poder Judicial y los justiciables, es que este documento se encuentra estructurado en las siguientes políticas generales de seguridad que consideran lo que se ha de tener en cuenta en la operatoria diaria a fin de lograr un mejor servicio de Justicia en la Provincia de San Luis y que se encuentran alineadas con la normativa *ISO/IEC 27002:2013*

1. **Políticas y estándares generales de seguridad para el personal judicial**
2. **Políticas y estándares de seguridad física y ambiental**
3. **Políticas y estándares de control para el acceso lógico**
4. **Políticas y estándares para la administración de los servicios y recursos informáticos**
5. **Políticas y estándares de cumplimiento y auditoría de los servicios informáticos**

Objetivo

Establecer y difundir las Políticas y estándares de Seguridad Informática a toda persona que utilice sistemas o servicios del Poder Judicial, y velar por los recursos informáticos de la institución, dando estricto conocimiento de las normas y custodia de los mismos.

Alcance

El acceso a los diferentes sistemas de información y/o tecnologías informáticas que existen o brinda 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 y toda persona que interactúe con cualquiera de los sistemas o servicios en todas sus circunscripciones, tanto se trate de magistrados, funcionarios, profesionales, administrativos, abogados, auxiliares de justicia, ciudadanos, pasantes, maestranza, servicios y cualquier otra persona que utilice elementos informáticos, sea cual fuere su nivel jerárquico, situación de revista o relación contractual que lo uniera con la institución.

Se aplicará a la utilización tanto de los sistemas de software, de los equipos informáticos hardware (computadoras, telefonía, impresoras, etc.), así como también 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, y las que surjan en razón de los continuos avances tecnológicos, quedará a consideración del Superior Tribunal de Justicia.

Justificación

La Secretaría de Informática Judicial, está facultada para definir **políticas y estándares** en materia informática, a fin de proponerlas al Superior Tribunal de Justicia.-

Compromiso

Es necesario que la Política de Seguridad sea parte de la cultura organizacional, por lo tanto se debe asegurar el compromiso de todos los comprendidos en la misma, para su difusión, consolidación y cumplimiento.

Beneficios

Las **Políticas de Seguridad Informática del Poder Judicial de la Provincia de San Luis** establecidas dentro de este documento son la base para la protección de los activos, sistemas y servicios tecnológicos e información del Poder Judicial del San Luis, permitiendo interactuar a las personas mediante procedimientos reglados, en un marco con normas claras y entendiendo que existen riesgos en el empleo de las TICs y que estos riesgos deben ser minimizados teniendo en cuenta y respetando los objetivos y necesidades institucionales del Superior Tribunal de Justicia en pos de la mejora continua del servicio de Justicia.

Sanciones por incumplimiento

El incumplimiento de la presente política podrá aparejar responsabilidad administrativa y/o penal (si el hecho además se encontrare comprendido en disposiciones del Código Penal), dependiendo de su naturaleza y gravedad, cuya sanción será aplicada por las autoridades competentes.

Desarrollo

1. **Políticas y estándares generales de seguridad para el Personal Judicial**

<u>POLÍTICA</u>: Todos los usuarios de los recursos y servicios informáticos se comprometen a conducirse bajo los principios de confidencialidad de la información y de uso adecuado de los recursos informáticos del PJSL, así como el estricto apego al presente manual de políticas y estándares de seguridad informática para usuarios.

1.1. Uso adecuado y confidencialidad

Es responsabilidad de los usuarios cumplir con lo establecido en la presente Política de Seguridad Informática y se deberán conducir conforme a los principios de confidencialidad de la información y uso adecuado de los recursos informáticos.

1.2. Entrenamiento en Seguridad Informática

Todo personal del PJSL de nuevo ingreso deberá conocer la presente Política de Seguridad Informática, debidamente publicada, donde se establecen las normativas mínimas respecto de los activos y servicios informáticos, las obligaciones para los usuarios y las sanciones que pueden aplicarse en caso de incumplimiento.-

El Superior Tribunal de Justicia a través del área que corresponda, asume el compromiso de realizar las capacitaciones o entrenamientos que se consideren pertinentes a fin de reforzar el proceso de mejora de la seguridad informática del PJSL.

1.3. Medidas disciplinarias

Cuando se identifique el incumplimiento a la presente política se remitirá el reporte o denuncia correspondiente al Superior Tribunal de Justicia o a la Oficina de Sumarios Administrativos, a sus efectos.-

1.4. Mecanismo de comunicación con la Secretaría de Informática Judicial (SIJ)

Cualquier tipo de pedido, solicitud de accesos, informes o requerimiento puntual que estuviese dirigido a la SIJ, el mismo y con carácter de obligatorio, deberá ser formulado vía oficio usando el sistema de gestión, o en su defecto mediante correo dirigido al e-mail institucional de la SIJ o de las respectivas ULG.

1° Circunscripción: informaticasl@justiciasanluis.gov.ar

2° Circunscripción: informaticavm@justiciasanluis.gov.ar

3° Circunscripción:

- Multifueros: informaticamf@justiciasanluis.gov.ar
- Concarán: informaticacon@justiciasanluis.gov.ar

En todos los casos, el pedido debe incluir una descripción de la necesidad con la debida justificación laboral y se debe efectuar desde la casilla de correo institucional personal del solicitante.

Para los casos puntuales de solicitudes de extensión o amplitud de “accesos ya otorgados”, habilitaciones especiales, permisos excepcionales, o situaciones análogas, el mismo deberá proceder de cualquiera de los funcionarios responsables del organismo solicitante.

En caso de que el requerimiento se efectuare en el marco de un proceso judicial, el mismo se dirigirá por sistema informático al Organismo de la SIJ.

2. Políticas y estándares de Seguridad Física y Ambiental

***POLÍTICA*: los mecanismos de control ambiental y acceso físico para el personal y terceros deben permitir el acceso a las instalaciones y áreas restringidas del PJSL, sólo a personas autorizadas para la salvaguarda de los equipos de cómputo y de comunicaciones, así como de las instalaciones en los diferentes Centros de Cómputo del Poder Judicial.**

2.1. Protección de activos informáticos

2.1.1. El usuario deberá reportar de forma inmediata a la SIJ y a la oficina que correspondiere, cuando detecte que existan riesgos reales o

potenciales para equipos de cómputo o comunicaciones, como pueden ser fugas de agua, de incendio, problemas eléctricos, etc.

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.

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 o en los recursos de red a los que el usuario tenga permiso de acceso.

2.2. Controles 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.

2.3. Ubicación y protección del equipamiento informático

2.3.1. 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.

2.3.2. Los usuarios NO deben mover o reubicar los equipos de cómputo o de telecomunicaciones, instalar o desinstalar software o periféricos, ni retirar sellos o fajas de los mismos sin la autorización de la SIJ, debiéndose solicitar a la misma en caso de requerir este servicio.

2.3.3. Mientras se opera el equipo de cómputo, no se deberán consumir alimentos o ingerir líquido alguno.

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

2.3.5. 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 SIJ a través de un plan detallado de movimientos debidamente autorizados por el titular del área que corresponda.

2.3.6. Queda totalmente prohibido que el usuario abra o desarme los equipos de cómputo (con ello se perdería la garantía que proporciona el proveedor de dicho equipo)

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

2.4. Mantenimiento del equipamiento informático

2.4.1. 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) 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 al personal técnico de la SIJ.

2.4.2. Los usuarios que requieran la instalación de software que no sea propiedad del PJSL, deberán justificar su uso y solicitar su autorización a la SIJ, indicando el equipo de cómputo donde se instalará el software y el período que permanecerá dicha instalación, siempre y cuando se acredite la titularidad del software previo a su instalación. Si ello se hubiese producido, personal asignado por la SIJ procederá de manera inmediata a desinstalar dicho software.

2.4.3. 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 PJSL, que no esté autorizado por la SIJ.

2.5. Copias de seguridad de la información

2.5.1. Los usuarios son los responsables de realizar copias periódicamente de la información sensible y crítica que se encuentre en sus computadoras personales o estaciones de trabajo, solicitando asesoría de la SIJ o al representante de ésta en su zona, para que dichos asesores determinen el medio en que se realizará dicho respaldo.

2.5.2. Los usuarios podrán solicitar, la realización de copias de resguardo de la información sensible o crítica en Infraestructura de la SIJ; para analizar la factibilidad de la solicitud se deberá indicar el tamaño de almacenamiento necesario aproximado, el tiempo en que interesa mantener el backup y los recursos disponibles para realizar dicha tarea.

2.6. Políticas de escritorios, pantallas limpias y ahorro energético

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:

- Almacenar en un mobiliario seguro bajo llave, cuando corresponda, los medios informáticos con información sensible o crítica del Organismo, cuando no están siendo utilizados y especialmente fuera del horario de Trabajo.
- Evitar dejar abiertos documentos, unidades de almacenamiento de datos y sesiones en 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.
- Para los casos que sea necesario realizar impresiones, se deberá retirar inmediatamente la información sensible o confidencial, una vez impresa la misma.
- Al finalizar la jornada laboral, el usuario deberá apagar la PC y el monitor asignado para ahorrar energía y evitar roturas de hardware ocasionados por cortes de energía imprevistos.

2.7. Ingreso y retiro de bienes informáticos

El ingreso o egreso de cualquier activo informático propiedad del Poder Judicial hacia/desde las instalaciones de trabajo deberá ser fundado e informado a la SIJ para que pueda autorizar el movimiento del mismo.

La conexión de cualquier equipo o periférico informático ajeno al Poder Judicial, no se podrá realizar sin previa justificación y autorización de la Secretaría de Informática Judicial.

3. Políticas y estándares de Control para el Acceso Lógico

<u>POLÍTICA</u>: 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) necesaria para acceder a la información y a la infraestructura tecnológica del PJSL, por lo cual deberá mantenerlo en forma confidencial.

3.1. Creación de cuentas de usuario y cuentas de correo

3.1.1. Para la solicitud de creación de cuentas se debe proceder acorde al apartado 1.4 de este documento.

3.1.2. El Superior Tribunal de Justicia de San Luis, es el único que puede otorgar la autorización para que se tenga acceso a la información que se encuentra en la infraestructura tecnológica del PJSL. Los permisos que se otorgan por defecto son los mínimos necesarios para el desempeño de sus funciones, con apego al principio “Necesidad de saber”, sin perjuicio de los permisos que corresponden a los Magistrados y Funcionarios en el ejercicio de la superintendencia, a los Funcionarios de la Secretaría de Informática Judicial y a los Agentes de la misma para el desempeño de sus funciones, incluyendo la administración de los sistemas.

3.1.3. Los funcionarios, magistrados o secretarios son los únicos que pueden solicitar la creación de cuentas de correo institucionales destinadas al funcionamiento interno del organismo en que desempeñan funciones.

3.1.3.1. Para la creación de cuentas institucionales propias del organismo, es obligatorio anexar al pedido de solicitud, dos responsables de la cuenta, un titular y un suplente, debiendo ambos firmar el convenio de uso del servicio asignado.

3.1.3.2. En caso de necesitar solicitar cuentas de empleados que prestan servicios temporarios, como pasantes u externos, es obligatorio anexar al pedido de solicitud, la fecha de expiración de

la cuenta. Solamente podrán solicitarlo para aquellos empleados que tienen a cargo.

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

3.1.5. Cada vez que sea necesario dar de alta un usuario/contraseña que permita acceder a cualquier activo informático, la SIJ deberá entregar al solicitante el convenio de uso y confidencialidad correspondiente, el cual deberá ser aceptado y firmado por parte del solicitante.

3.1.6. No deben existir usuarios de uso genérico para el puesto de trabajo.

3.2. Administración y uso de contraseñas

3.2.1. El uso de la contraseña para acceso a la red y la contraseña para acceso a sistemas, debe ser realizado de forma individual y no debe compartirse dicho recurso a tercero alguno.

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

3.2.3. La obtención o cambio de una contraseña se debe hacer de forma segura, acreditándose el usuario ante la SIJ como empleado del PJSL o con el documento de identidad que permita identificarlo.

3.2.4. 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.

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

- Debe ser una combinación de al menos 3 de las siguiente 4 condiciones

  Mayúsculas – Minúsculas – Números -Caracteres especiales**:**[1]

- Debe contener como mínimo 8 caracteres de longitud.

- No puede incluir el nombre de usuario o parte de los nombres personales.
- Deben ser difíciles de adivinar, esto implica que las contraseñas no se deben relacionar con el trabajo o la vida personal del usuario (no debe hacer referencia a ningún concepto, objeto o idea reconocible).
- Deben ser diferentes a las contraseñas que se hayan usado previamente.

3.2.6. El usuario debe cambiar inmediatamente la contraseña que se le es asignada por primera vez y, consecuentemente, actualizarla en periodos que no excedan los 3 meses independientemente si el sistema obliga o no a efectuar dicha actualización.

3.2.7. El usuario dueño de la cuenta podrá solicitar personalmente el cambio o reseteo de la contraseña ante la SIJ, siendo la nueva contraseña asignada del tipo temporaria y debiendo el usuario cambiarla inmediatamente post reseteo.

3.2.8. Todo usuario que tenga la sospecha de que su contraseña es conocida por otra persona, tendrá la obligación de cambiarla inmediatamente.

3.2.9. La inhabilitación o bloqueo de usuarios, ya sea en carácter definitivo o temporario, podrá ser solicitado según el apartado 1.4 del presente documento, por cualquier funcionario que tenga como responsable al usuario en cuestión o por la máxima autoridad del área a la cual pertenece el usuario.

3.3. Responsabilidades

3.3.1. Todos los usuarios son responsables del identificador de usuario y contraseña que recibe para el uso y acceso de los recursos informáticos asignados

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

3.3.3. 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 que se deba facilitar para la reparación o mantenimiento de algún sistema o equipo siendo esta la única alternativa posible. Para este caso, el usuario antes de entregar el equipo deberá cambiar su contraseña por una temporaria para facilitar el acceso al personal técnico o informático el cual deberá estar debidamente identificado y 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.

3.3.4. 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.

3.4. Administración de privilegios

3.4.1. Cualquier cambio en los roles y responsabilidades de los usuarios que modifique sus privilegios de acceso a la infraestructura tecnológica del PJSL, deberá ser notificado por escrito o vía correo electrónico a la SIJ con el visto bueno del titular del área solicitante, para realizar el ajuste solicitado.

3.4.2. Tratamiento de los permisos asignados.

- Por cada servicio o asignación directa de recurso/permiso informático en caso de movimiento del empleado por rol funcional o de área, la SIJ procederá a revocar o conceder los permisos a los recursos informáticos basándose en los comunicados o acuerdos del

STJ, salvo que se indique mantener algún permiso durante la transición vía nota remitida a la SIJ según mecanismo de comunicación 1.4.

- Para los casos de “Jubilación”, “Cargo por mayor jerarquía” y “Renuncia laboral”, la SIJ debe revocar todos los accesos del empleado y dar de baja la cuenta a partir de la fecha publicada de baja de empleado. Solo para aquellos empleados con modalidad “***Retiro Voluntario”***, se dejará habilitada la cuenta solamente para poder consultar el recibo de sueldo a través de SIAJUS, el resto de los servicios se darán de baja inmediatamente.

3.5. Control de accesos remotos

3.5.1. Está prohibido el acceso a redes externas por vía de cualquier dispositivo, cualquier excepción deberá ser documentada y contar con la aprobación de la SIJ.

3.5.2. 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 SIJ.

3.6. Controles de acceso lógico

3.6.1. El acceso a la infraestructura tecnológica del PJSL para personal externo debe ser informado por escrito o sistema y autorizado al menos por un titular de área del PJSL.

3.6.2. Está prohibido que los usuarios utilicen la infraestructura tecnológica informática para obtener acceso no autorizado a la información u otros sistemas de información del PJSL.

3.6.3. Todos los usuarios deberán autenticarse por los mecanismos de control de acceso provistos por la SIJ antes de poder usar la infraestructura tecnológica del PJSL.

3.6.4. Los usuarios no deben proporcionar información de los mecanismos de control de acceso a las instalaciones e infraestructura tecnológica

del PJSL a personal alguno, a menos que se tenga autorización de la SIJ

3.6.5. 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.

4. Políticas y estándares para la administración de los servicios y recursos informáticos

<u>POLÍTICA</u>: Los usuarios deberán utilizar los recursos o servicios informáticos de la infraestructura del Poder Judicial de la Provincia de San Luis teniendo en cuenta las normas y procedimientos institucionales para proteger la información que en ellos residen, la SIJ debe velar por el buen uso de los recursos maximizando la calidad de servicio brindado a la justicia.

4.1. Asistencia informática general

4.1.1. EL usuario dispondrá de manuales y tutoriales en la sección de informática del sitio web institucional del PJSL para las consultas de las problemáticas más habituales.

4.1.2. Los usuarios deberán canalizar las peticiones de asistencia al área técnica dependiente de la SIJ o en su defecto proceder según apartado 1.4 del presente documento (mecanismo de comunicación).

4.2. Software y hardware en los puestos de trabajo

4.2.1. El software que deberá instalarse por defecto en todos los equipos del PJSL 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.
- Software de soporte para firma digital.
- Todo software o sistema desarrollado o autorizado por la SIJ.

El hardware de cada organismo será recibido bajo firma por el responsable del mismo, conforme a las obligaciones que al respecto prevé la Ley Orgánica de Administración de Justicia. Periódicamente se actualizará el inventario que lleva la SIJ, debiendo suscribir tal responsable la documentación pertinente.

4.2.2. 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/hardware 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, se deberá contar con la correspondiente autorización de la SIJ y del responsable del organismo.

4.2.3. En caso de que el puesto de trabajo sea compartido por más de un usuario, cada cual deberá acceder al equipo con un usuario propio e inequívoco, de forma tal que si existiese un incidente se pueda identificar al responsable del mismo.

4.2.4. Equipo desatendido

Los usuarios deberán mantener sus equipos de cómputo con controles de acceso mínimos, como bloqueo de sesión con contraseña y protectores de pantalla, como una medida de seguridad cuando el usuario necesita ausentarse de su puesto de trabajo por un tiempo.

4.3. Reserva de sala de capacitación informática

Para solicitar el servicio de reserva de sala se deberá proceder según el Protocolo de uso para las aulas/salas de Capacitación vigente a la fecha de solicitud.

4.4. Gestión y difusión de información en los portales webs institucionales.

Cada sección o apartado de los sitios webs institucionales deberá tener un responsable titular y suplente designado, cuya función será de mantener actualizado las diferentes secciones que tenga a cargo.

4.5. Servicio de videoconferencias

Para solicitar el servicio de videoconferencia se deberá cumplimentar el Protocolo de uso para Videoconferencias vigente a la fecha de solicitud.

4.6. Servicio de Telefonía

4.6.1. La SIJ es encargada de mantener el servicio de telefonía IP y además de actualizar el display y la configuración de los teléfonos IP. La información al respecto a colocar en la página web institucional es responsabilidad de la Oficina de Protocolo y Ceremonial.

4.6.2. Los usuarios deberán proceder según apartado 1.4 cada vez que necesiten lo siguiente:

- Cambiar información sobre el interno
- Realizar un movimiento del teléfono
- Requerir alguna funcionalidad especial, la cual podrá ser brindada, previo análisis de factibilidad técnica.

4.7. Servicio de sistema de expedientes electrónicos

Para todo lo relacionado al sistema informático de gestión judicial, el usuario debe cumplimentar el “Reglamento General del Expediente Electrónico” vigente a la fecha.

4.8. Servicio de Justicia para usuarios externos.

A los usuarios externos, les serán aplicables en lo pertinente las disposiciones de la Política de Seguridad, con las siguientes particularidades:

4.8.1. Creación de cuentas de usuario y cuentas de correo

4.8.1.1. El Superior Tribunal de Justicia de San Luis, es el único que puede otorgar la autorización para que se tenga acceso a la información que se encuentra en la infraestructura tecnológica del PJSL.

4.8.1.2. Los Abogados, Auxiliares de Justicia y los Ciudadanos pueden solicitar la creación de cuentas de correo institucionales destinadas al funcionamiento de los sistemas, notificaciones y todo acto administrativo o jurídico que el PJSL disponga.

4.8.1.3. La SIJ sólo será la responsable de la creación de cuentas institucionales, y los propios Organismos serán los responsables de la vinculación electrónica de los usuarios en los expedientes y el control de visualización y acceso a los mismos.

Estos domicilios electrónicos (cuentas de correo) son únicas, intransferibles e indelegables.

4.8.2. Administración y uso de contraseñas

4.8.2.1. Cuando un usuario olvide, bloquee o extravíe su contraseña, deberá reportarlo por escrito a la SIJ, indicando esta situación reportando los módulos de sistemas, servicios o sistemas, para los que se requiere una nueva contraseña, siendo el usuario responsable de las acciones que se hayan realizado durante este tiempo. La SIJ podrá solicitar la documentación personal que estime acorde a fin de verificar la persona que demanda dicho servicio.

4.8.2.2. El cambio de una contraseña se debe hacer de forma segura, a través del sistema correspondiente.

4.8.2.3. Está prohibido que los identificadores de usuarios y contraseñas se encuentren de forma visible en cualquier medio

impreso o escrito, de manera de que se permita a personas no autorizadas su conocimiento.

4.8.2.4. La inhabilitación o bloqueo de usuarios, ya sea en carácter definitivo o temporario, será efectuada cuando sea ordenado por la SIJ por razones de servicio, por el STJSL o cuando mediare sanción de inhabilitación en la matrícula por el tribunal de ética del colegio profesional pertinente fehacientemente comunicada a la SIJ.

4.8.3. Responsabilidades

Ningún usuario debe usar la identificación, identidad, firma digital o contraseña de otro usuario, aunque dispongan de la autorización del propietario (esta acción es considerada falta grave e ilegal).

4.8.4. Administración de privilegios

La SIJ al emitir los accesos a los sistemas y servicio los realizará en base a los privilegios y roles que cuente el usuario para tal fin conforme lo establece el Reglamento General de Expediente Electrónico.

4.8.5. Control de accesos remotos

Está prohibido para la SIJ el acceso remoto a equipos de trabajos de usuarios externos para realizar cualquier tipo de tarea, constatación o diagnóstico por parte del PJSL.

4.8.6. Asistencia informática general

4.8.6.1. EL usuario dispondrá de manuales, tutoriales, cursogramas, diagramas de flujos, videos, etc. en la sección de informática del sitio web institucional del PJSL para las consultas de las problemáticas más habituales.

4.8.6.2. Los usuarios deberán canalizar las peticiones de asistencia o reportes de inconvenientes a la SIJ procediendo según el apartado 1.4 del presente documento (mecanismo de comunicación).

Los reclamos se considerarán válidos y se dará curso a los mismos cuando se utilicen los canales que la SIJ ofrece para tal fin, los que serán publicados en el sitio web institucional de la Secretaría.

Sólo se atenderán reclamos por problemas informáticos, quedando excluidos del mismo, problemas administrativos y de procedimiento judicial, los cuales deberán ser evacuados por los organismos pertinentes.

4.8.6.3. La SIJ brindará a los usuarios externos información adicional que permita identificar fehacientemente al usuario si el problema se suscita en la infraestructura del servicio brindado, ya que no prosperarán reclamos por problemas individuales en los equipos de trabajos de los usuarios externos, esto fuera por falta de componentes, versionados o distribuciones no recomendadas, o cualquier diferencia entre el software o hardware recomendado y el instalado.

4.8.7. Recomendaciones sobre el Software y hardware utilizado en los puestos de trabajo de los usuarios externos

4.8.7.1. El software que deberá instalarse en los puestos de trabajos de los usuarios externos para el uso de los sistemas del PJSL será el siguiente y de responsabilidad exclusiva, excluyente y obligatoria del usuario:

- Sistema Operativo
- Antivirus
- Suite de ofimática recomendada por la Secretaría de Informática Judicial (SIJ).
- Software de soporte para firma digital.

4.8.7.2. Empleo de software y hardware adicional:

El usuario será el único responsable de la instalación de cualquier tipo de paquetes de software adicional o hardware al recomendado para el trabajo con sistemas del PJSL.

Si los mismos generan conflicto con los sistemas o servicios que brinda el PJSL para el despliegue de la función judicial el usuario será el único responsable de solucionar el estado de conflicto. Además deberá velar por mantener acorde a las recomendaciones de la SIJ los programas de aplicación y componentes según las versiones o distribuciones recomendadas.

4.9. Servicio de Carpetas Compartidas o acceso de archivos en red.-

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. La creación de carpetas compartidas implica almacenamiento a emplear en los servidores por lo cual en el pedido se deberá estimar el crecimiento aproximado de la carpeta y además será necesario indicar los usuarios que accederán a la carpeta y el tipo de acceso deseado para c/usuario (ej.; lectura o escritura de archivos).

4.10. Servicio de correo electrónico

4.10.1. Los interesados en acceder al servicio de correo se deberán presentar ante la SIJ para solicitar la generación de una casilla de correo electrónico y de una clave de acceso a la misma.

4.10.2. Será responsabilidad de cada usuario del servicio de correo, evitar la sobrecarga de las distintas bandejas de sus casillas de correo, de manera que estén siempre en condiciones de recibir nuevas comunicaciones.

4.10.3. El usuario de correo dispondrá para consulta generales en el sitio web institucional del PJSL, distintos tutoriales de configuraciones y mejores prácticas relacionadas al servicio de correo electrónico.

4.10.4. 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 PJSL, a menos que cuente con la autorización del titular del área solicitante.

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

4.10.6. 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 SIJ.

4.10.7. El PJSL se reserva el derecho de acceder y revisar las comunicaciones de correo electrónico, solo para aquellos casos en que se ha verificado que se ha comprometido la seguridad o se ha violado alguno de los apartados de la presente política de Seguridad Informática.

4.10.8. Para los ataques de spam desde cuentas internas institucionales y sabiendo que el correo electrónico por naturaleza es de acceso libre se procederá de la siguiente forma:

Habiéndose comprobado que para realizar el ataque se ha utilizado una cuenta de correo interna y, por lo tanto, se han expuesto las credenciales (usuario/contraseña) del usuario al intruso y siendo que la SIJ debe velar por el bienestar de todos los recursos informáticos y accesos a los sistemas, la SIJ procederá a deshabilitar inmediatamente la cuenta para frenar la intrusión perpetrada por el atacante. Una vez contenido el siniestro se deberá notificar al responsable de la cuenta atacada con los pasos recomendados a seguir.

La deshabilitación de la cuenta sólo impide el acceso a los servicios que requieran autenticación con la misma sin afectar el funcionamiento

del servicio en sí. Por ejemplo, para el caso particular del correo, la deshabilitación de la cuenta sólo impide el acceso a la cuenta sin afectar la recepción de correos en la misma.

4.10.9. El usuario debe de utilizar el correo electrónico del PJSL, 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.

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

4.11. Servicio de Internet

4.11.1. El acceso a internet provisto a los usuarios del PJSL es exclusivamente para las actividades relacionadas con las necesidades del puesto y función que desempeña.

4.11.2. Todos los accesos a internet tienen que ser implementados a través de las redes internas del PJSL.

4.11.3. La asignación del servicio de internet, deberá solicitarse por escrito acorde al mecanismo de comunicación con la SIJ (apartado 1.4).

4.11.4. 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 SIJ.

- Saben que queda totalmente prohibido el uso de software o metodologías para evitar o saltar los controles de navegación existentes.

4.11.5. La utilización de internet es para el desempeño de su función y puesto en el PJSL y no para propósitos personales.

4.11.6. Los esquemas de permisos de acceso a internet se dividen en 2 niveles:

NIVEL 1: Acceso Empleados: es el acceso que poseen todos los empleados judiciales y se habilita por defecto en el puesto de trabajo. Este acceso consiste en una amplia lista de sitios gubernamentales, de información jurídica, jurisprudencia, organizaciones sin fines de lucro, sitios académicos, de investigación o educativos y relativos a toda la actividad judicial.

NIVEL 2: Acceso Funcionario: Es el acceso ampliado de navegación y solo se restringen las "***restricciones globales"*** que se le aplican al servicio. Este nivel se otorga por defecto a todos los secretarios, funcionarios y magistrados del STJ, además a profesionales universitarios y prosecretarios siempre que el acceso sea necesario y esté directamente relacionado con la función que desempeña, debiendo presentar respecto de estos últimos la nota correspondiente según apartado 1.4 del presente documento.

4.11.7. Excepciones de accesos a Internet

Pueden existir casos particulares de habilitaciones a páginas no habilitadas en cada uno de los 2 niveles de navegación de internet existente, dicha solicitud deberá ser justificada y solicitada a la SIJ según apartado 1.4 del presente documento.

4.11.8. Restricciones Globales

El servicio de internet tiene restricciones globales que se aplican en toda la red y para los 2 NIVELES DE ACCESO, siendo de dos tipos, a saber:

- Automático: es un bloqueo dinámico y automático basado en categorías y en listas de reputaciones mundiales (pornografía, sitios de streaming de multimedios, de descargas, phishing, virus, armas, drogas, etc.)
- Manual: la SIJ mantiene una lista de accesos prohibidos que se adicionan a los bloqueos automáticos. Este tarea se hace manualmente en base al monitoreo de accesos del servicio.

5. Políticas y estándares de cumplimiento y auditoría del uso de los servicios informáticos

POLÍTICA: Fijar los controles mínimos, bases y normativas para la política de Seguridad Informática teniendo en cuenta el funcionar diario y los avances tecnológicos del Poder Judicial de la provincia de San Luis en post de la mejora continua del proceso judicial y el servicio al ciudadano.

5.1. Derechos de Propiedad Intelectual

5.1.1. Está prohibido por las leyes de derechos de autor y por el PJSL, realizar copia no autorizadas de software, ya sea adquirido o desarrollado por el PJSL.

5.1.2. Los sistemas desarrollados por personal, interno o externo, que sea parte de la SIJ, o sea coordinado por ésta, son propiedad intelectual del PJSL.

5.1.3. Está prohibido acceder al código fuente de un software sin autorización explícita del autor.

5.2. Uso Aceptable de los servicios o recursos informáticos

5.2.1. 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.

5.2.2. 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 se podrá hacer siempre que el recurso se encuentre disponible y no exista otro usuario que precise emplear el recurso para sus tareas laborales.

5.2.3. 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.

5.2.4. 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 o de la SIJ.

5.2.5. 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 PJSL.

5.3. Usos Prohibidos de los servicios o recursos informáticos

5.3.1. Transgredir o eludir las verificaciones de identidad u otros sistemas de seguridad.

5.3.2. Leer información o archivos de otros usuarios sin su permiso.

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

5.3.4. Lanzar, activar, ejecutar cualquier tipo de software/hardware o acceder a páginas web que generen una degradación o denegación de cualquiera de los servicios o activos informáticos.

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

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

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

5.3.8. 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.

5.3.9. 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.

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

5.3.11. 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.

5.3.12. Obtener cualquier tipo de ganancia económica personal.

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

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

5.3.15. Conectar cualquier dispositivo de red (access point, notebook, netbook, tablet, impresora, scanner, router, switch, cámara de seguridad, etc.) a las redes cableadas e inalámbricas de todos los edificios propiedad del poder judicial sin previa autorización de la SIJ.

5.3.16. Emplear chips y dispositivos USB de conexión a internet no propietario del Poder Judicial sin previa autorización de la SIJ, se

procederá a la remoción directa en caso de detectarse su uso sin la debida autorización.

5.3.17. Conectar cualquier dispositivo móvil (celulares) o de multimedia NO propietario del poder judicial en la estación de trabajo, ya sea para carga de batería, acceso al contenido del dispositivo, etc.

5.3.18. 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.

5.3.19. Introducir en los Sistemas de Información o la red contenidos obscenos, amenazantes, inmorales u ofensivos.

5.3.20. Utilizar cualquier sistema de correo o cualquier tipo de comunicación electrónica con el propósito de revelar información privada de otras personas, sin su consentimiento o divulgar información confidencial del PJSL

5.3.21. 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.

5.3.22. Los usuarios de las áreas del PJSL no deben establecer redes de área local, conexiones remotas a redes internas o externas, intercambio de información con otros equipos de cómputo empleando la infraestructura de red del PJSL, sin la autorización por escrito de la SIJ.

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

5.3.24. Está prohibido el uso de herramientas de hardware o software para violar los controles de seguridad informática.

5.3.25. Ningún usuario ni empleado del PJSL 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 SIJ.

5.3.26. 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 SIJ.

5.3.27. Ningún usuario debe intencionalmente escribir, generar, compilar, copiar, propagar, ejecutar o tratar de introducir código de computadora diseñado para auto replicarse, 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 PJSL. El incumplimiento de este estándar será considerado una falta grave.

5.4. Gestión de incidentes

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

5.4.2. 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 a su superior inmediato.

5.4.3. Cualquier incidente generado durante la utilización u operación de los activos de tecnología de información del PJSL, debe ser reportado a la SIJ para que se proceda lo más rápido posible a la resolución del mismo.

5.5. Controles contra Softwares Maliciosos

5.5.1. Para prevenir infecciones por virus informáticos, los usuarios del PJSL, deben evitar hacer uso de cualquier clase de software que no haya sido proporcionado y validado por la SIJ.

5.5.2. Los usuarios del PJSL, 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 SIJ.

5.5.3. El usuario debe verificar mediante el software de antivirus autorizado por la SIJ 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.

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

5.5.5. Debido a que algunos virus son extremadamente complejos, ningún usuario del PJSL debe intentar erradicarlos de las computadoras. Lo adecuado/correcto es llamar al personal de la SIJ para que sean ellos quienes lo solucionen.

5.6. Revisiones del cumplimiento

5.6.1. La SIJ realizará acciones de verificación del cumplimiento de las presentes Políticas de Seguridad Informática.

5.6.2. La SIJ 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.

5.7. Monitorización

5.7.1. 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.

5.7.2. 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.

5.7.3. 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.

Referencias

1. Los caracteres especiales permitidos son: **( ) ` ~ ! @ # $ % ^ & * - + = | \ { } [ ] : ; " ' < > , . ? /**

Definiciones y Acrónimos

SIJ: Secretaría de Informática Judicial

STJ: Superior Tribunal de Justicia

PJSL: Poder Judicial de la Provincia de San Luis

TICs: Tecnologías de la Información y comunicación

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.

Incidente de Seguridad: Un incidente de seguridad es un evento adverso en un sistema de computadoras, o red de computadoras, que puede comprometer o compromete la confidencialidad, integridad y/o disponibilidad de la información. Puede ser causado mediante la explotación de alguna vulnerabilidad o un intento o amenaza de romper los mecanismos de seguridad existentes

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 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.

Fuentes y normativas consultadas

- ✓ Acuerdo 338/2011-Primeras Políticas de Seguridad de los Recursos Informáticos – Poder Judicial de San Luis
- ✓ Acuerdo Nº 263/2015 –Reglamento General de Expediente Electrónico con las últimas Políticas de Seguridad de los Recursos Informáticos – Poder Judicial de San Luis

- ✓ Disposición 3/2013 – Administración Publica Nacional – “Política de Seguridad de la Información Modelo”
- ✓ Normativa publicada por ICIC – Programa Nacional de Infraestructuras Criticas de Información y Ciberseguridad de la República Argentina
- ✓ 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.