Resistencia, 31 de enero de 2022. LY

**Nº 9**

**V I S T O:**

El ataque sufrido en algunos servidores del Poder Judicial de la Provincia del Chaco por un malware del tipo ransomware y las Resoluciones dictadas en consecuencia Nº 3/2022, Nº 4/2022 y Nº 7/2022; y

**C O N S I D E R A N D O:**

I. Que, conforme se consignara en la Resolución Nº 3/2022, el día domingo 9 de enero de 2022 se tomó conocimiento y se confirmó, a través del informe del Director de la Dirección de Tecnologías de la Información, un ataque sufrido en algunos servidores por un malware del tipo ransomware.

II. Que, de hecho, en ese momento se constituyó un Comité de Crisis, integrado por las señoras Ministras y los señores Ministros del Superior Tribunal de Justicia, el Secretario de Superintendencia y el Director de la Dirección de Tecnologías de la Información.

III. Que, en dicho instrumento, se dispuso que "*el Director de la Dirección de Tecnologías de la Información, Armando Daniel Chapo, brinde un informe escrito pormenorizado y circunstanciado, con carácter urgente y en el plazo máximo de veinticuatro (24) horas, indicando, con los datos con los que cuente aunque sean parciales, el origen del ataque, los hechos acontecidos, las medidas tomadas para minimizar riesgos y las consecuencias y el alcance de los daños relevados*".

IV. Que, asimismo, se encomendó "*al Secretario de Superintendencia Provisorio, Lisandro Yolis, y/o al Director de la Dirección de Tecnologías de la Información, Armando Daniel Chapo, la realización de las denuncias administrativas y penales ante organismos oficiales nacionales y/o provinciales correspondientes*".

V. Que, en concreto, se dispuso que "*a través de la Dirección de Tecnologías de la Información, la suspensión de todos los servicios de índole digital (INDI, IURE, IURE -Ingreso de demandas-, SIGI, SIGI profesional, servidores, internet, conexiones de red, conexiones VPN, correos oficiales, domicilios electrónicos, y todo otro servicio digital que brinda el Poder Judicial) hasta el domingo 16 de enero de 2022, con informes periódicos*".

VI. Que, además, se solicito "*a los y las auxiliares de la justicia, Consejo y Colegios de Abogados y Abogadas de toda la Provincia, dependencias de los Ministerios Públicos Fiscal y de la Defensa, el resguardo de cualquier documento o archivo digital con que cuenten, en caso de que sea necesaria su presentación ante los organismos intervinientes por posibles pérdidas*".

VII. Que, todo ello fue comunicado y difundido, dadas las limitaciones tecnológicas, por whatsapp y redes sociales personales y del Centro de Estudios Judiciales, el mismo día domingo 9 de enero a las 22 horas aproximadamente.

VIII. Que, el día lunes 10 de enero, el Director de la Dirección de Tecnologías de la Información elevó al Superior Tribunal de Justicia un informe confidencial y reservado.

IX. Que, en el mencionado informe, se detalla que "*el día sábado 8 de enero de 2022 en las primeras horas de la mañana, se recibió un aviso de no funcionamiento del Lex Doctor por parte de una usuaria. En principio, se atribuyó a inconvenientes locales de conexión. A medida mañana del mismo día, aproximadamente a las 10hs, se recibió un aviso de no funcionamiento del SIGI desde el interior de la Provincia. En consecuencia, se dispuso la revisión y restablecimiento del servicio. El técnico encargado de la recuperación informó que no estaba funcionando el servicio de cluster de los servidores y que los servidores no respondían. Luego, de*

*varios intentos por casi una hora (siendo las 11hs aproximadamente), se logró ingresar a uno de los servidores, reponer el servicio de cluster detenido y ver la estructura del servidor. En ese momento, el técnico informa que podría ser una infección, recibiendo una advertencia del antivirus, y, siendo aproximadamente las 14hs, se determinó que se trataría de un malware del tipo ransomware. Aproximadamente a las 15hs, se comenzaron a desconectar los servicios de red para aislar el problema y suspender posibles infecciones o propagación del virus, suspensión de cuentas afectadas en active directory, cambio y renovación de contraseñas de administradores, y dando de baja todos los servicios. Además, se detectaron procesos maliciosos, lo cuales fueron detenidos y eliminados. En un primer análisis que se hizo ese mismo día, se determinó la infección en varios servidores virtualizados (SQL Server). También se verificaron los sitios de back up, que, en general, se encontraban afectados en la misma medida. Los trabajos se concluyeron aproximadamente a las 22hs. (...) el día domingo alrededor de las 20hs, se realizó el reporte del incidente en la Dirección Nacional de Ciberseguridad (CERT.ar) dependiente de la Jefatura de Gabinete de Ministros de la Nación*", consignándose, además, todos los trabajos que se realizaron y los contactos que se mantuvieron con especialistas nacionales y provinciales.

X. Que, el día martes 11 de enero, Daniel Chapo y Lisandro Yolis, junto con el Fiscal en turno, Doctor Roberto Villalba, efectuaron la denuncia penal ante la Dirección de la Policía de Investigaciones - Departamento de Cibercrimen.

XI. Que, también el día martes 11 de enero aproximadamente a las 10 horas, el Superior Tribunal de Justicia emitió un comunicado y lo difundió, dadas las limitaciones tecnológicas, por whatsapp y redes sociales personales y del Centro de Estudios Judiciales, sobre las gestiones realizadas "*para el libramiento de las órdenes de pago pendientes, mediante un acceso que ha brindado la Empresa ECOM*", indicando que, "*en*

*la medida de las posibilidades en tanto las limitaciones existentes, se comenzarán a realizar los pagos de sumas de capital, interés y honorarios en las causas judiciales*".

XII. Que, por Resolución N° 4/2022, se dispuso "*la prórroga de la suspensión de servicios digitales más allá del 16 de enero de 2022, informándose oportunamente la forma y tiempos de restablecimiento de dichos servicios*" y, a los fines de la determinación del origen del ataque, se contrató a la empresa Penta Security Solutions S.R.L. para la emisión de un informe de carácter confidencial para el Superior Tribunal de Justicia.

XIII. Que, en la mencionada resolución, se expresa que "*el día domingo 9 de enero, el Poder Judicial sufrió un ataque de un malware del tipo ransomware*" y que "*desde esa fecha, se constituyó un Comité de Crisis integrado por las Ministras y los Ministros del Superior Tribunal de Justicia, el Secretario de Superintendencia y el Director de la Dirección de Tecnologías de la Información, el cual se encuentra trabajando constantemente en el análisis y evaluación de la situación. Que, dicho Comité ha mantenido reuniones con la Dirección Nacional de Ciberseguridad de la Jefatura de Gabinete de Ministros de la Nación y con expertos nacionales y provinciales en la materia, recibiendo asesoramiento para afrontar de la mejor manera posible el ataque. Que, dichos expertos han recomendado la realización de un peritaje informático para la determinación de los hechos que dieron origen a esta situación. Que, en ese contexto, el Comité de Crisis se encuentra trabajando decidida e ininterrumpidamente para dar una solución lo más pronta posible, sin embargo y dados los plazos solicitados por las empresas proveedoras, entiende prudente para garantizar la nuevas medidas de seguridad requeridas prorrogar la suspensión de servicios digitales más allá del 16 de enero de 2022, informándose oportunamente la forma y tiempos de restablecimiento de dichos servicios. Que atento a lo expuesto, la Dirección de Tecnologías de la Información solicita la contratación de un servicio de*

*consultoría en investigación de incidentes de ciberseguridad, a fin brindar informe sobre el origen del ataque y las consecuencias y el alcance de los daños relevados*".

XIV. Que, ello fue comunicado y difundido anticipadamente, dadas las limitaciones tecnológicas, por whatsapp y redes sociales personales y del Centro de Estudios Judiciales, el día miércoles 12 de enero a las 14 horas aproximadamente.

XV. Que, el día miércoles 19 de enero aproximadamente a las 18 horas, el Superior Tribunal de Justicia emitió un comunicado y lo difundió, dadas las limitaciones tecnológicas, por whatsapp y redes sociales personales y del Centro de Estudios Judiciales.

XVI. Que, en dicho comunicado, se consigna que "*los integrantes del Comité de Crisis (...) continúan, en largas jornadas, con los trabajos sobre el ataque de un malware que sufrió el Poder Judicial de la Provincia del Chaco. En ese sentido, se ha contratado a Penta Security Solutions para la realización de una consultoría en investigación sobre el incidente de ciberseguridad. Al respecto, en el día de la fecha, la empresa especializada en seguridad ha brindado un primer informe preliminar y ha mantenido una reunión de la que participaron la Presidenta, Emilia María Valle, la Ministra Iride Isabel María Grillo, el Ministro Víctor Emilio Del Rio, los Secretarios de Superintendencia, el Director de la Dirección de Tecnologías de la Información y Pablo Huerta por parte de la empresa para explicación detallada, al quien se le solicitó una ampliación y profundización en algunos aspectos del informe, lo cual será entregado a la brevedad. En dicho informe, se explica que el ataque se produjo por un grupo delictivo denominado 'Hive Ransomware' que habría comenzado sus operaciones ilegales en junio de 2021, señalando que la variante de virus utilizado en el ataque al Poder Judicial data recién de enero de 2022, lo cual, por su actualidad, vulnera la mayoría de las protecciones de seguridad (entre ellas,*

*los antivirus). Asimismo, en el mencionado informe, se destaca que ese grupo delictivo realiza, primero, tareas de investigación sobre las medidas de protección y el funcionamiento de los sistemas del organismo, posteriormente elimina los registros de firewall y desactiva los antivirus, para, recién luego, lanzar el ataque con código malicioso; con este complejo accionar torna imprevisible el ataque y tiene un alto poder destructivo. En este contexto, el Comité de Crisis se encuentra trabajando en la readecuación de los protocolos de ciberseguridad, para ello se está manteniendo contacto con expertos provinciales y nacionales, con funcionarios de la Dirección Nacional de Ciberseguridad y se ha contratado a una empresa también especializada Z Consulting, para avanzar sobre el reforzamiento y refuncionalización de la infraestructura tecnológica, como así también sobre reevaluación de las estrategias de backup. Por otra parte y en tanto que el ataque no se limitó a la información sino que toda la infraestructura del Poder Judicial ha sido atacada -lo cual implica en los hechos una revisión individual de cada uno de los servidores y de cada una de las máquinas de escritorio (más de 3.500 en toda la Provincia) como así también la reinstalación de todos los sistemas y programas para evitar residuos del código malicioso o puertas traseras de acceso-, el Comité se encuentra avanzado para iniciar un gradual y paulatino restablecimiento de los servicios digitales generales en las próximas semanas para los organismos de feria y, de esta forma, encontrarse en condiciones de iniciar las actividades judiciales luego de la feria; por lo tanto, oportunamente se informarán los levantamientos de servicios, mientras tanto se mantendrán suspendidos los siguientes: INDI, IURE, IURE -Ingreso de demandas-, SIGI, SIGI profesional, servidores, internet, conexiones de red, conexiones VPN, correos oficiales, domicilios electrónicos. Desde otra perspectiva, la Dirección de Tecnologías de la Información, junto con la empresa proveedora Veeam, está avanzando sobre el análisis de los backups y el recupero de la información. En concreto y en virtud de lo expuesto, se pone*

*en conocimiento sobre cada una de las Circunscripciones Judiciales: Primera Circunscripción Judicial (Resistencia): por la cantidad de información, aún se encuentra en etapa de relevamiento y recuperación de la información. Sin embargo, se otorgaron accesos limitados a redes a los Juzgados de feria y a la Dirección General de Administración para garantizar el funcionamiento de actividades esenciales y de carácter alimentario -por ejemplo, pagos de capital e intereses a justiciables, honorarios profesionales, ejecución presupuestaria y liquidación de haberes-. Segunda Circunscripción Judicial (Presidencia Roque Sáenz Peña): por la cantidad de información, aún se encuentra en etapa de relevamiento y recuperación de la información. Sin embargo, se han comenzado a restablecer algunos servicios de gestión local de expedientes. Tercera Circunscripción Judicial (Villa Ángela), Cuarta Circunscripción Judicial (Charata), Quinta Circunscripción Judicial (General San Martín), Sexta Circunscripción Judicial (Juan José Castelli): se relevaron mínimas pérdidas de información y se han comenzado a restablecer servicios de gestión local de expedientes. En consecuencia, se solicita y recuerda el resguardo de cualquier documento o archivo digital con que cuenten, en caso de que sea necesaria su presentación ante los organismos intervinientes por posibles pérdidas. En consideración de información inexacta o malintencionada, el Superior Tribunal de Justicia recalca que el único canal de información oficial son los comunicados de prensa y entrevistas personales de funcionarios autorizados, y que, como ya se ha dicho y se ha visto en las últimas horas, muchas empresas y organismos públicos han sufrido ataques similares por esto u otro tipo de malware y que es sabido que la tecnología avanza vertiginosamente y que, lamentablemente, este tipo de acciones maliciosas y delictuales procura para alcanzar sus fines avanzar más rápido que las soluciones y las inversiones que están al alcance para afrontarlos. Finalmente, el Superior Tribunal de Justicia hace saber que, además de la reuniones técnicas y de avance, el día de mañana se reunirá, a las 10hs, con*

*los Colegios y Consejo de Abogados y Abogadas de toda la Provincia y, a las 11hs, con la Asociación de Magistrados y Funcionarios Judiciales, la Entidad de Magistrados y Funcionarios de la Justicia de Paz y Faltas y con representantes de los cuatro gremios que nuclean a los agentes; a los fines de informar el estado de situación y evacuar dudas al respecto".*

XVII. Que, en su informe, la empresa Penta Security Solutions consigna que "*entre el viernes 7 de enero de 2022 y el viernes 8 de enero de 2022 se produjo una infección por ransomware sobre los equipos informáticos del Poder Judicial de la Provincia del Chaco. El ransomware que afectó a la institución, se encuentra asociado al grupo 'Hive Ransomware'. Se posee un registro sobre su primera actividad en junio de 2021, el cual afectó el sistema de salud en los Estados Unidos (en particular el Memorial Health System); interrumpiendo la atención médica y poniendo en riesgo la vida de varios pacientes. Esto puso en evidencia la falta de escrúpulos de este tipo de grupo ciberdelictivo. A fines de junio 2021, se dio a conocer el ataque a Altus Group, una compañía canadiense de tecnología. En noviembre 2021, salió a la luz una nueva víctima pero en otro continente, Media Markt, el minorista de electrónica de consumo más grande de Europa. Se cree que este grupo está brindando su código malicioso en una modalidad de RaaS (Ransomware as a Service) poniendo a disposición en la comunidad de ciberdelincuentes la posibilidad de utilizar su ransomware para perpetuar ciberataques. El historial del accionar de este grupo y la posibilidad de estar brindando su código malicioso como un servicio a la comunidad de ciberdelincuentes, abre un amplio foco de ataque en donde cualquier organismo (tanto público como privado) puede ser víctima de ciberdelincuentes. Una de las características más destacables de este ransomware es que detiene la ejecución de: • programas que realizan copias de seguridad y restauración de computadoras, • antivirus, • antispyware, • copias de archivos en segundo plano. De manera adicional, ejecuta actividades de borrador de registros;*

*técnica común utilizada para reducir la evidencia forense disponible. El 'Hive ransomware' se basa en métodos comunes de compromiso inicial, que incluyen: • equipos vulnerables, • credenciales VPN comprometidas, • correos electrónicos de phishing. En el caso del Poder Judicial de la Provincia del Chaco se identificó la variante '7j45q'; asociada con eventos de Enero 2022*".

XVIII. Que, como hipótesis de la forma de ataque, el informe indica que "*un agente externo relacionado con 'Hive ransomware Group', logró acceder a la infraestructura de la institución por medio del servidor de correo electrónico expuesto en Internet (...). Se introdujo malware en el servidor HV05 para establecer una conexión continua con la red de la institución. Luego de realizar una tarea de comprensión de la infraestructura y obtener credenciales administrativas, se planificó la ejecución de la infección de ransomware para el viernes a la noche*".

XIX. Que, como conclusión, se expresa que "*la pandemia Covid-19 ha forzado tanto al ámbito privado como al público en la aceleración de puesta a disposición de tecnología en Internet para facilitar lo que se conoce como teletrabajo o homeoffice. Muchas infraestructuras tecnológicas no pensadas hasta ese momento para realizar un cambio en la forma de acceso aceleraron su adaptación; exponiéndose a situaciones que nunca antes fueron tenidas en cuenta. De la misma forma que las instituciones y organismos se volcaron al uso masivo de Internet, los delincuentes también afectados por el encierro; comenzaron a mutar sus actividades delictivas al ciberespacio. De una manera igual, o incluso en algunos casos más rápida, se puede ver hoy en día el crecimiento de ciertos grupos ciberdelictivos que aprovechan esta transición de las organizaciones y entidades para producir ilícitos. El Poder Judicial de la Provincia del Chaco fue víctima de una variante enero 2022 de ransomware asociada a un grupo en crecimiento constante desde junio de 2021: 'Hive ransomware group'. El ataque del malware ransomware, iniciado el viernes 7 de enero por la noche, es la*

*materialización de la planificación de una actividad delictiva que tuvo como mínimo inicio el jueves 6 de enero. Al no disponer de registros que permitan comprender el ataque inicial, lo más probable es que se haya comprometido el servicio de correo electrónico al encontrarse expuesto en Internet. Cabe mencionar que, el mismo viernes durante el día, ya habían comenzado actividades de actualizaciones de los programas por parte del equipo técnico. Es necesario recordar que, hoy en día, el uso de la tecnología antivirus no garantiza la protección contra infecciones de tipo 'Zero Day'. El trabajo activo de la ciberseguridad se vuelve una necesidad en toda organización y organismo. Ante la agilidad y masividad del uso de la tecnología, se recomienda implementar un proceso de monitoreo continuo de las buenas prácticas de ciberseguridad y concientización a los usuarios de la tecnología. Retomando la realidad que nos toca hoy en día respecto a la pandemia y la nueva variante Ómicron... De la misma forma que estar vacunado contra el Covid-19 reduce las posibilidades de contagio y mortalidad, aunque podría no evitar su contagio y trasmisión. El uso de soluciones de seguridad no garantiza la no materialización de incidentes de ciberseguridad. Es importante destacar que ningún método es 100% efectivo, pero sí es vital su uso*".

XX. Que, el día miércoles 26 de enero aproximadamente a las 18 horas, el Superior Tribunal de Justicia emitió un comunicado y lo difundió, dadas las limitaciones tecnológicas, por whatsapp y redes sociales personales y del Centro de Estudios Judiciales.

XXI. Que, en el mencionado, se expresa que "*con el informe de Penta Security Solutions sobre la investigación del incidente de ciberseguridad y acelerando el proceso de inversión en readecuación de la infraestructura, la Dirección de Tecnologías de la Información ha trabajado denodadamente con la empresa proveedora Veeam en el recupero de los backups afectados, en virtud de haber oportunamente contratado a dicha*

*empresa con la previsión de un soporte técnico a distancia y con las herramientas tecnológicas que brinda. En consecuencia y hasta este momento, se ha logrado recuperar la siguiente información contenida en bases de datos y sistemas del Poder Judicial: Al 7 de enero de 2022, en toda la Provincia, Sistema de Gestión Penal (SIGI) y el servidor de aplicaciones. Al 6 de enero de 2022, Sistemas de Gestión, bases de datos y todos los documentos y archivos de IMF-IMCIF, Gabinete Científico, Compras y Suministros, Secretaría General de Archivo. Al 1 de enero de 2022, los tres (3) laboratorios de desarrollo de software de la Dirección de Tecnologías de la Información. Al 25 de diciembre de 2021, la Página Web del Poder Judicial. Al 20 de noviembre de 2021, Sistemas de Gestión Lex Doctor de organismos jurisdiccionales y no jurisdiccionales. Al 20 de noviembre de 2021, todos los documentos y archivos de las oficinas que integran el Poder Judicial dentro de la red interna en Resistencia. Al 13 de noviembre de 2021, Sistemas de Gestión Lex Doctor del Fuero de Niñez, Adolescencia y Familia -Civil- de Resistencia. Al 4 de septiembre de 2021, en toda la Provincia, Sistemas y Bases de Datos de Ingreso Digital de Escritos (INDI), Control de Trámites y Notificaciones, Sistema de Boleta de Tasa de Justicia, Sistema de Consultas de Saldos Bancarios, Certificados de Deuda, Base de Datos de Matrícula de Abogados y Abogadas, Registro de Usuarios de Profesionales, Libro de Registro de Sentencias. Al 4 de septiembre de 2021, Sistema de Oficina de Mandamientos y Notificaciones, Registro Digital de Asistencia (RDA), Sistema de Turnos de Defensorías Oficiales, consulta de candidatos y jurados elegidos, padrón de peritos, Sistema de Gestión de la Dirección General de Personal. En otro orden, el Superior Tribunal de Justicia se encuentra en proceso de elaboración de un Protocolo de Contingencia para el inicio de las tareas el 1 de febrero de 2022, evaluando una posible suspensión de términos y audiencias para el relevamiento y reconstrucción de información en los organismos y a fin de otorgar a los profesionales un tiempo para adaptarse*

*a dicho protocolo de contingencia y garantizar su labor. Todo esto ha sido informado en sendas reuniones mantenidas por el Superior Tribunal de Justicia, primero, con los Presidentes de los Colegios y Consejo de Abogadas y Abogados de toda la Provincia, y, luego, con la Asociación de Magistrados y Funcionarios Judiciales, la Entidad de Magistrados y Funcionarios de la Justicia de Paz y Faltas y con representantes de los cuatro gremios que nuclean a los agentes*".

XXII. Que, además de los comunicados emitidos, tanto la Presidenta del Superior Tribunal de Justicia como el Secretario de Superintendencia brindaron sucesivas entrevistas a medios de comunicación, a fin de mantener actualizada la información sobre la situación.

XXIII. Que, en virtud de las recomendaciones recibidas por expertos nacionales y provinciales, como así también por funcionarios de la Dirección Nacional de Ciberseguridad (CERT.ar) dependiente de la Jefatura de Gabinete de Ministros de la Nación, se inició un proceso de fortalecimiento y reforzamiento de la infraestructura tecnológica afectada, la reingeniería de dicha infraestructura y la readecuación de las políticas de seguridad y ciberseguridad del Poder Judicial a las nuevas amenazas existentes, con las contrataciones de servicios y las respectivas compras.

XXIV. Que debe recordarse que el ataque fue perpetrado por un grupo denominado "Hive Ransomware", con carácter delictual y malicioso, mediante una versión de un virus sumamente virulento y novedoso creado en enero de 2022, por lo cual logró vulnerar las medidas de seguridad del Poder Judicial, eliminando registros de firewall, desintalando o desactivando los antivirus y afectando toda la infraestructura tecnológica y, principalmente, back ups y servidores.

XXV. Que, este Superior Tribunal de Justicia debe destacar la labor y el compromiso de cada uno de los y las integrantes del Poder

Judicial que han prestado funciones durante estas últimas semanas y solicitar el trabajo mancomunado de todas las personas internas y externas que coadyuvan al desarrollo del servicio de justicia para salir adelante de esta situación que nos ha perjudicado a todos (agentes, auxiliares de la justicia, justiciables y ciudadanía).

XXVI. Que, es preciso señalar que la Dirección de Tecnologías de la Información ha trabajado denodadamente con la empresa proveedora Veeam en el recupero de los backups afectados, en virtud de haber oportunamente contratado a dicha empresa con la previsión de un soporte técnico a distancia y con las herramientas tecnológicas que brinda.

XXVII. Que, en virtud de todo lo expuesto y dadas las circunstancias, este Superior Tribunal de Justicia considera necesario, propicio y prudente el dictado de un protocolo de contingencia para el restablecimiento gradual y progresivo de los servicios y sistemas y para determinar los lineamientos de trabajo para el Poder Judicial a partir del 1 de febrero de 2022, de conformidad con las facultades de superintendencia conferidas por la Constitución de la Provincia del Chaco, artículo 162, inciso 7, y la Ley 1-B Orgánica del Poder Judicial, artículo 25, inciso 13.

Por ello, el **SUPERIOR TRIBUNAL DE JUSTICIA**,

**RESUELVE:**

**I. APROBAR** el Protocolo de Contingencia para el restablecimiento gradual y progresivo de los servicios y sistemas y para determinar los lineamientos de trabajo para el Poder Judicial a partir del 1 de febrero de 2022 que como ANEXO forma parte de la presente.

**II. DISPONER**, a través del Centro de Estudios Judiciales, la realización de las capacitaciones necesarias para la explicación del Protocolo de Contingencia tanto para agentes del Poder Judicial como para auxiliares de la justicia.

**III.** **ENCOMENDAR** a la Secretaría de Superintendencia y a la Dirección de Tecnologías de la Información, junto con las Salas del Superior Tribunal de Justicia, la colaboración con los organismos jurisdiccionales y no jurisdiccionales en todas aquellas cuestiones referidas al Protocolo de Contingencia.

**IV.** **REMITIR** copia de la presente al Poder Ejecutivo Provincial, al Poder Legislativo Provincial, a la Procuración General, a la Defensoría General y a la Fiscalía que se encuentra interviniendo en la denuncia formulada.

**V.** **REGISTRAR** y comunicar.

Dr. ALBERTO MARIO MODI
J U E Z
SUPERIOR TRIBUNAL DE JUSTICIA

EMILIA MARIA VALLE
PRESIDENTA
SUPERIOR TRIBUNAL DE JUSTICIA

VICTOR EMILIO DEL RIO
J U E Z
SUPERIOR TRIBUNAL DE JUSTICIA

ADE ISABEL MARIA GRILLO
J U E Z
SUPERIOR TRIBUNAL DE JUSTICIA

FOLKERTO IGNACIO TOLLO
J U E Z
SUPERIOR TRIBUNAL DE JUSTICIA

**ANEXO RESOLUCIÓN N° 9/2022**

**PROTOCOLO DE CONTINGENCIA Y LINEAMIENTOS DE TRABAJO PARA EL PODER JUDICIAL DE LA PROVINCIA DEL CHACO**

**Artículo 1. Vigencia.**

El presente protocolo de contingencia entrará en vigencia el 1 de febrero de 2022 e irá perdiendo aplicación a medida que se logren restablecer los servicios y sistemas del Poder Judicial.

A esos fines el Superior Tribunal de Justicia, a través de la Dirección de Tecnologías de la Información o de la Secretaría de Superintendencia, informará el restablecimiento gradual de los servicios y sistemas.

**Artículo 2. Servicios digitales básicos.**

La Dirección de Tecnologías de la Información restablecerá los servicios digitales básicos y urgentes en los organismos jurisdiccionales y no jurisdiccionales, además, se limitarán ciertos pasos dentro del proceso de digitalización.

**Artículo 3. Expediente Mixto.**

Durante la vigencia del presente protocolo y hasta tanto se restablezcan los servicios y sistemas que por el presente se limitan, se implementará el Expediente Mixto previsto en el artículo 25 del Reglamento de Expediente Electrónico que como Anexo I forma parte de la Ley 3286-M.

En ese sentido, se conjugará un proceso mixto entre digital y papel, debiendo las presentaciones realizarse en formato papel -conforme artículo 11 del presente-, tramitarse internamente a través de los sistemas de gestión habilitados, emitiéndose los actos con firma electrónica dentro de dichos

sistemas y con firma ológrafa fuera de ellos para su notificación y cumplimiento.

A medida que se restablezcan gradual y progresivamente los servicios y sistemas, se irán habilitando los pasos digitales limitados y el expediente electrónico, reduciendo de esta manera el impacto del proceso de transición.

**Artículo 4. Servicios externos.**

La Dirección de Tecnologías de la Información deshabilitará accesos para personas externas al Poder Judicial al SIGI, IURE, INDI, Domicilios Electrónicos y de otros servicios brindados a través de la página web (www.justiciachaco.gov.ar).

Una vez garantizada la seguridad y estabilidad de la infraestructura, restablecerá gradualmente dichos servicios externos.

**Artículo 5. Servicios internos.**

La Dirección de Tecnologías de la Información concederá acceso interno a los sistemas de gestión y al correo electrónico -sólo como servicio de mensajería interna- a los organismos jurisdiccionales y no jurisdiccionales.

Asimismo, limitará el servicio de internet y de otros servicios brindados a través de la página web (www.justiciachaco.gov.ar), concediendo únicamente acceso limitado a internet a las personas encargadas de comunicaciones jurisdiccionales urgentes, pagos en expedientes, liquidación de haberes y ejecución presupuestaria.

Cuando la seguridad y estabilidad de la infraestructura lo permita, otorgará gradualmente acceso a los demás servicios.

**Artículo 6. Suspensión general de términos y audiencias.**

Disponer la suspensión general de términos y audiencias en toda la Provincia desde el 1 de febrero de 2022 y hasta el 13 de febrero de 2022 -inclusive-.

**Artículo 7. Suspensión especial de términos y audiencias.**

Una vez finalizada la suspensión general estipulada en el artículo 6, a pedido de una de las partes o de oficio, se podrán interrumpir o suspender plazos procesales en un expediente en particular, cuando por la afectación total o parcial de la información, el acto sea de imposible o de muy difícil cumplimiento (por aplicación del principio emanado del último párrafo de artículo 173 del Código Procesal Civil y Comercial de la Provincia del Chaco).

**Artículo 8. Suspensión de términos y audiencias por organismo.**

Sin perjuicio de lo previsto en el artículo 7 y en el supuesto de considerarse necesario, Magistrados y Magistradas podrán solicitar al Superior Tribunal de Justicia la suspensión de términos y audiencias para ese organismo específicamente y por un plazo determinado.

**Artículo 9. Trámites urgentes. Otros trámites.**

Sin perjuicio de la suspensión general de términos y audiencias dispuesta en el artículo 6, siempre que las limitaciones en los servicios y sistemas y cuando las piezas procesales necesarias no se hayan perdido, los organismos deberán tramitar y resolver todas aquellas cuestiones urgentes, comprendiendo, entre otros supuestos, la realización de gestiones impostergables, tramitación de procesos urgentes, tramitación de causas con personas privadas de la libertad, emisión de órdenes de pago y cualquier otro trámite que pueda implicar la pérdida de un derecho o un perjuicio grave.

Además, los organismos deberán llevar adelante todas aquellas tareas que no se vean afectadas por la limitación del acceso a los servicios y sistemas o que puedan realizarse porque no se hayan perdido actos o piezas procesales.

**Artículo 10. Presentaciones. Criterio General.**

Las presentaciones de demandas o escritos de inicio se realizarán en formato papel en las Mesas Receptoras Informatizadas correspondientes o en el organismo jurisdiccional competente donde no existan aquellas.

Las demás presentaciones se realizarán en formato papel en el organismo correspondiente.

En todos los casos, los organismos deberán tramitarlos a través de los sistemas de gestión, a efectos de dar continuidad al expediente electrónico, cuando se pueda restablecer su funcionamiento pleno -conforme artículo 3 del presente-.

Una vez garantizada la seguridad y estabilidad de la infraestructura, se restablecerá gradualmente la presentación digital de demandas y escritos.

**Artículo 11. Notificaciones.**

Las notificaciones de providencias, resoluciones y sentencias se realizarán por nota o por cédula o por cualquier otro método no digital o electrónico autorizado por el código procesal aplicable -según corresponda-.

**Artículo 12. Atención telefónica.**

A los fines de evitar la concurrencia innecesaria, todos los organismos tienen la obligación de brindar información telefónica a auxiliares de la justicia, justiciables y a la ciudadanía en general, siempre que la consulta refiera a información de acceso público y el o la solicitante acredite un interés legítimo a criterio del organismo en obtener la información.

**Artículo 13. Consulta de saldos de cuentas bancarias.**

Hasta tanto se puedan restablecer los servicios externos y sin perjuicio de la posibilidad de concurrir directamente al Nuevo Banco del Chaco, se podrá solicitar en formato papel en el Departamento de Control Financiero de la

Dirección General de Administración o vía correo electrónico -saldoscuentasjudiciales@gmail.com- el informe de saldos de cuentas bancarias.

El o la solicitante deberá indicar correctamente los datos del expediente, carátula, organismo jurisdiccional y número de cuenta.

El Departamento de Control Financiero de la Dirección General de Administración emitirá -en papel o vía correo electrónico- el informe, en un plazo estimado de veinticuatro (24) horas hábiles.

**Artículo 14. Listas de despacho. Difusión.**

Hasta tanto se puedan restablecer los servicios externos, la Secretaría de Superintendencia dará a difusión, a través de correo electrónico -stjchaco@gmail.com- o vía whatsapp, las listas de despacho de todos los organismos jurisdiccionales de la Provincia, cuyo procedimiento específico será comunicado por el Superior Tribunal de Justicia.

Sin perjuicio de ello, en la medida de las posibilidades, se habilitarán otros canales de difusión, lo cual será comunicado oportunamente por el Superior Tribunal de Justicia.

**Artículo 15. Guía Judicial.**

Hasta tanto se puedan restablecer los servicios externos, la Secretaría de Superintendencia dará a difusión, a través de correo electrónico -stjchaco@gmail.com- o vía whatsapp, la Guía Judicial de toda la Provincia, cuyo procedimiento específico será comunicado por el Superior Tribunal de Justicia.

Sin perjuicio de ello, en la medida de las posibilidades, se habilitarán otros canales de difusión, lo cual será comunicado oportunamente por el Superior Tribunal de Justicia.

**Artículo 16. Concurrencia. Presencialidad.**

En virtud de la suspensión de servicios externos -conforme artículo 4 del presente- y hasta tanto se puedan restablecer los mismos, auxiliares de la justicia, justiciables y cualquier otra persona interesada deberá concurrir de forma presencial a los organismos a fin de tomar vista de los expedientes.

En consecuencia, se exigirá la exhibición del Pase Sanitario o Carnet Físico de Vacunación o PCR negativo de las últimas setenta y dos (72) horas para el ingreso a los edificios o dependencias y el estricto cumplimiento de las medidas sanitarias vigentes, especialmente, uso de barbijo, distanciamiento social e higiene de manos.

Finalmente, se recuerda a los y las agentes del Poder Judicial la vigencia de las Resoluciones N° 444/2021, N° 620/2021 y N° 816/2021, con las limitaciones tecnológicas del presente protocolo y con las actualizaciones de medidas sanitarias dictadas por la autoridad de aplicación.

**Artículo 17. Reconstrucción.**

Supeditado a los recuperos de información que informe la Dirección de Tecnologías de la Información, cada organismo iniciará un proceso de relevamiento, análisis y reconstrucción de los expedientes o actuaciones administrativas, de conformidad con las pautas generales brindadas por el artículo 145 del Código Procesal Civil y Comercial de la Provincia del Chaco y Capítulo X de la Ley 179-A Código de Procedimientos Administrativos -según corresponda-, y bajo los lineamientos especiales que a continuación se establecen.

En virtud de la excepcionalidad de la situación, para el inicio del proceso de reconstrucción, el organismo dispondrá y solicitará a todas las partes intervinientes, en el plazo uniforme y conjunto de diez (10) días hábiles, la presentación en formato papel de todos los escritos, antecedentes y actos del

organismo que se encuentre en su poder o que hayan sido recuperados de los sistemas, debidamente ordenados cronológicamente.

Efectuadas las presentaciones por todas las partes intervinientes, se otorgará a las mismas un plazo uniforme y conjunto de diez (10) días hábiles para que se expidan acerca de la autenticidad de las copias incorporadas.

Por su parte, el Secretario o la Secretaria del organismo deberá agregar copias de todos los instrumentos con los que cuente la dependencia.

En caso de ser necesario, de encontrarse disponible en los sistemas y en la medida de las posibilidades, la Dirección de Tecnologías de la Información podrá brindar información para la validación de los actos y piezas a reconstruir.

Cumplidos los pasos precedentemente expuestos, la Magistratura dictará resolución teniendo por reconstruidos los expedientes o actos procesales, continuando con el Expediente Mixto.

Durante el proceso de reconstrucción y hasta el dictado de la resolución final, todos los plazos y audiencias del expediente se encontrarán suspendidos.

En relación a los archivos digitales, los organismos deberán determinar los actos o piezas procesales perdidas, según las fechas de implementación de los sistemas y el grado de digitalización en cada uno de dichos organismos, como así también los posibles recuperos de información que ha llevado adelante la Dirección de Tecnologías de la Información.

Estas pérdidas digitales incluyen, entre otras, actos emitidos por los organismos, notificaciones electrónicas, presentaciones efectuadas a través de los sistemas y cualquier otro acto que haya sido realizado únicamente mediante medios electrónicos o sistemas.

No se considerarán perdidos aquellos actos o piezas procesales a las que se pueda tener acceso por otros medios -verbigracia, impresiones realizadas por el organismo, presentaciones o documentos en formato papel-.

**Artículo 18. Principios rectores.**

En caso de duda y por la excepcionalidad de la situación, los organismos deberán inclinarse por la interpretación que mejor garantice el ejercicio de los derechos.

En relación con el proceso de reconstrucción y en caso de duda, los organismos deberán inclinarse por la interpretación a favor de la existencia y del recupero de los actos y piezas procesales.

En virtud de la particular situación, corresponde exigir a todas las personas internas o externas al Poder Judicial el especial cumplimiento del principio de buena fe y lealtad procesal durante la vigencia del presente protocolo de contingencia.

**Artículo 19. Situaciones no previstas.**

Todas aquellas situaciones no previstas en el presente protocolo de contingencia, deberán ser planteadas por escrito en formato papel ante el Superior Tribunal de Justicia.