ADM 11857/22
“PROTOCOLO DE ACUERDOS 2022”

ACUERDO N° 85-STJSL-SA.- En la Provincia de San Luis, a DOCE días del mes de ABRIL de DOS MIL VEINTIDÓS, los Sres. Ministros del Superior Tribunal de Justicia, Dres. ANDREA CAROLINA MONTE RISO, CECILIA CHADA, JORGE OMAR FERNÁNDEZ y JORGE ALBERTO LEVINGSTON.-

DIJERON: Visto que desde el 3 de abril de 2017, se implementó la tramitación despapelizada del expediente electrónico en todo el ámbito del Poder Judicial Provincial, conforme fuera dispuesto mediante Acuerdo Nº 61/2017, punto II.-

Que tal forma de tramitación de los expedientes electrónicos ha quedado incorporada en el art. 104 de la nueva Ley Orgánica de la Administración de Justicia de la Provincia Nº IV-0086-2021 y en las nuevas normativas procesales, en el marco de la Reforma Judicial que como política de Estado ha adoptado la Provincia.-

Que ante la mayor disponibilidad de servicios digitales, es necesario establecer y mantener las medidas pertinentes para la debida protección activa y preventiva de los activos, sistemas y servicios tecnológicos e información del Poder Judicial de San Luis, con recursos humanos que coadyuven a sostener en el tiempo su confidencialidad, integridad y disponibilidad.-

Que en tal sentido, el art. 106 de la citada Ley establece:

“ARTÍCULO 106.- El Superior Tribunal de Justicia dispondrá y mantendrá actualizadas Políticas de Seguridad Informática, que sean la base para la protección de los activos, sistemas y servicios tecnológicos e información del Poder Judicial de San Luis, debiendo contener como mínimo:

a) Políticas y estándares generales de seguridad para el personal judicial;

b) Políticas y estándares de seguridad física y ambiental;

c) Políticas y estándares de control para el acceso lógico;

d) Políticas y estándares para la administración de los servicios y recursos informáticos;

e) Políticas y estándares de cumplimiento y auditoría de los servicios informáticos.-

Asimismo, se adoptarán por el Poder Judicial procedimientos y tecnologías de respaldo o duplicación, a fin de asegurar la inalterabilidad y seguridad de los sistemas informáticos y la continuidad de los servicios, los que serán determinados por la Secretaría de Informática Judicial periódicamente conforme a la disponibilidad de tecnologías. A esos fines, se efectuarán las previsiones presupuestarias correspondientes".-

Que en el art. 47 de la misma Ley se establecen las atribuciones y funciones de la Secretaría de Informática Judicial, y en el último párrafo de tal artículo se dispone que para el cumplimiento de sus funciones cuenta con Subsecretarías, Delegaciones, Departamentos, Áreas y Subáreas que cumplirán las tareas que se les asigne, en el marco de las que se establecen en el presente Artículo, y contará con las estructuras de personal, todo conforme a los cargos asignados por la Ley de Presupuesto, todo ello según se determine por Acuerdo del Superior Tribunal de Justicia.-

Que en el ultimo Organigrama de tal Secretaría, aprobado por Acuerdo N° 550/2019, la Seguridad Informática se atribuye a un Departamento dependiente de la Sub Secretaría de Tecnología, lo que es pertinente reestructurar en virtud del crecimiento actual de requerimientos de seguridad, que la misma tiene que ser considerada transversal a la organización, y de los citados avances tecnológicos afrontados por el Poder Judicial, por lo que debe responder directamente a los Responsables de la Secretaría de Informática Judicial.-

Que asimismo, respecto del anterior Organigrama, se ha advertido la necesidad de que un cargo vacante en mesa de ayuda Segundo nivel del Departamento Sistema de Gestión Judicial se redistribuya en la nueva Sub Secretaría de Seguridad Informática, por lo que no se añaden nuevos números de cargos.-

Por ello, y conforme a lo dispuesto por el art. 39 inc. 7 ptos. b y c de la Ley Orgánica de la Administración de Justicia;

ACORDARON: I.- APROBAR el nuevo Organigrama de la Secretaría de Informática Judicial del Superior Tribunal de Justicia y las atribuciones y funciones de su Sub Secretaría de Seguridad Informática, conforme Anexos I y II del presente Acuerdo, quedando modificado en lo pertinente el Reglamento del Proceso de Informatización del Poder Judicial de la Provincia de San Luis, aprobado por Acuerdo N° 415/2017.-

II.- DEJAR sin efecto el Acuerdo N° 550/2019, manteniendo la distribución actual de funciones entre los Secretarios de tal Organismo, correspondiendo a la Dra. Sandra Zulema Romero Guzmán la Sub Secretaría de Administración y ULG II, y al Dr. Alejandro David Flores Dutrús la Sub Secretaría de Tecnología y ULG III, a quien además se le asigna la Sub Secretaría de Seguridad Informática.-

III.- DISPONER que los llamados a ascensos a las nuevas categorías que se prevén en la Estructura del Organigrama aprobado en el pto. I, se harán efectivos en oportunidad de los ascensos generales para Profesionales, y que para acceder a cargos superiores se especificarán, en cada caso, los perfiles técnicos que se requerirán.-

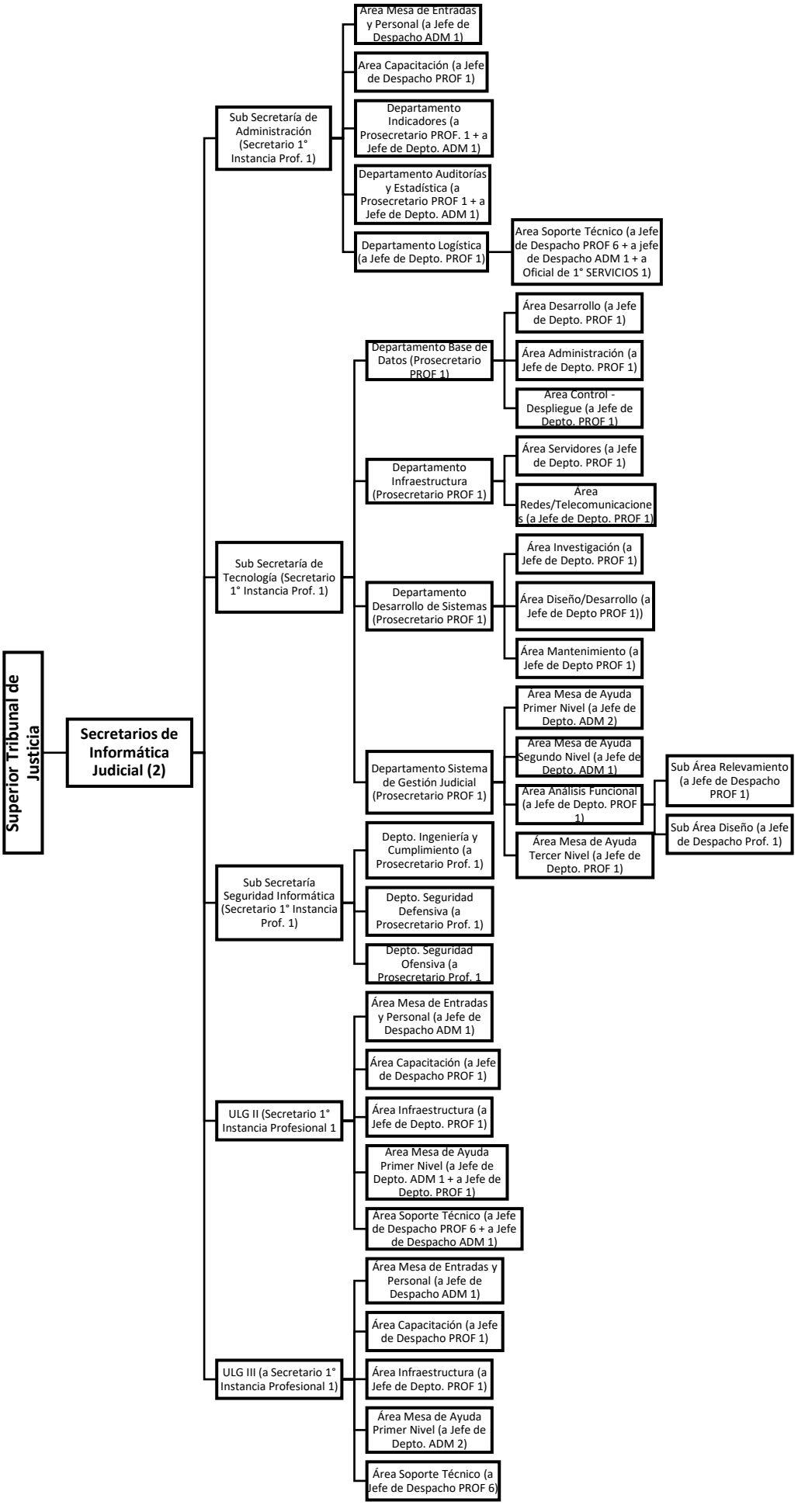
IV.- ORDENAR que por Dirección de Recursos Humanos se publique el presente Acuerdo en la página web institucional del Poder Judicial en el link “Acuerdos”, y en el Boletín Oficial y Judicial de la Provincia, por un día.-

Con lo que se dio por terminado el presente acto, disponiendo los Señores Ministros se comunique a Secretaría de Informática Judicial, se agregue copia del presente Acuerdo en ADM 12302/22, y que vuelva el mismo a Dirección de Recursos Humanos.-

SIJ

ANEXO I

ORGANIGRAMA DE LA SECRETARÍA DE INFORMÁTICA JUDICIAL



Anexo II

Atribuciones y Funciones de la Sub Secretaría de Seguridad Informática

La SUBSECRETARIA de SEGURIDAD INFORMATICA estará a cargo de:

a) Coordinar y dirigir los departamentos a cargo, Ingeniería y Cumplimiento, Seguridad Defensiva y Seguridad Ofensiva respectivamente.
b) Comunicar y capacitar en los temas relacionados en Seguridad Informática.
c) Planificar, coordinar y dirigir en las tres circunscripciones actividades que involucren nuevas políticas o cambios de infraestructura y seguridad en la red interna.
d) Promover el cumplimiento a la política de seguridad informática, asesorar y acompañar en el proceso de formulación de políticas y normativas de seguridad en todas las áreas de la Secretaría informática y supervisar su cumplimiento.
e) Participar asesorando en los procesos de compras de equipamiento, procurando la mayor eficiencia y compatibilidad con las políticas fijadas.
f) Promover la aplicación de auditorías enfocadas a la seguridad y ejecución constante de planes de evaluación de seguridad.
g) Elaborar reportes de amenazas, filtraciones e intentos del no cumplimiento de la política de seguridad
h) Mantener comunicación permanente con organismos judiciales o áreas informáticas externas con el propósito de asesoramiento mutuo, intercambio de información y experiencias.

El Depto. de Ingeniería y Cumplimiento tendrá a su cargo:

a) Análisis y reingeniería de malware
b) Auditoría de servicios
c) Investigación de soluciones de seguridad y mejores prácticas en medidas de seguridad
d) Armados de ambientes de pruebas para los distintos sistemas del PJSL.
e) Mantener actualizadas las políticas de seguridad de información
f) Diseñar protocolos, guías y procedimientos de Seguridad
g) Implementar, gestionar y mantener actualizada las políticas de backups
h) Diseñar y mantener los planes de contingencia de los sistemas críticos del PJSL

El Depto. Seguridad Defensiva tendrá a su cargo:

a) Administración de las distintas soluciones de seguridad
b) Mantener y segurizar los distintos sistemas o servicios existentes del PJSL
c) Mantener y aplicar acciones preventivas sobre los sistemas segurizados
d) Detección de amenazas ocultas, generación de planes de threat hunting.
e) Securización del entorno y operatividad de las salas de servidores de la Institución

f) Implementar barreras físicas y procedimientos de control, como medidas de prevención y contramedidas ante amenazas a los activos informáticos tanto desde fuentes externas como internas.

El Depto. Seguridad Ofensiva tendrá a su cargo:

a) Planificar y ejecutar continuamente planes de evaluación de seguridad contra los distintos sistemas o soluciones existentes
b) Generación de informes y propuestas de mejoras de seguridad
c) Capacitaciones y planes de concientización orientados en seguridad
d) Ejecutar periódicamente simulacros de ataques de seguridad