ACORDADA Nº 32/2023 EXPEDIENTE Nº 5932/2023

Corte Suprema de Justicia de la Nación

Buenos Aires, 2 de noviembre de 2023.-

Los Señores Ministros que suscriben la presente,

CONSIDERARON:

I) Que en el contexto actual de digitalización y modernización, los procesos judiciales y administrativos enfrentan desafíos sin precedentes, siendo las amenazas cibernéticas una de las principales preocupaciones, dada su capacidad para comprometer la integridad, confidencialidad y disponibilidad de los sistemas informáticos del Tribunal.

II) Que la Corte Suprema de Justicia de la Nación, como custodio de información crítica y sensible, tiene la responsabilidad ineludible de garantizar la resiliencia y protección de sus sistemas informáticos frente a cualquier amenaza cibernética.

III) Que diversos organismos estatales han reconocido la importancia de la ciberseguridad fortalecido su estructura con departamentos y áreas dedicadas exclusivamente,

reflejando la imperiosa necesidad de esta función en el ámbito público.

IV) Que es imperativo, en respeto a la autonomía del Poder Judicial, diseñar y adoptar estrategias, protocolos y medidas específicas para abordar los desafíos actuales y futuros en ciberseguridad que afecten directamente a la Corte Suprema de Justicia de la Nación.

V) Que la gestión proactiva de riesgos, la respuesta ágil a incidentes y la formación continua en ciberseguridad son esenciales para garantizar la protección integral de nuestros activos digitales y la confianza pública en el sistema judicial.

VI) Que, dada la sofisticación y evolución constante de las amenazas informáticas, es esencial contar con un equipo especializado en ciberseguridad, capacitado y actualizado conforme a las mejores prácticas, normativas y estándares internacionales en materia de seguridad informática.

VII) Que la supervisión constante de la operatividad, seguridad y resiliencia de los sistemas informáticos de la Corte Suprema de Justicia de la Nación es

fundamental para garantizar el acceso efectivo a la justicia, proteger los derechos fundamentales de los ciudadanos y fortalecer el Estado de Derecho en un entorno digital.

VIII) Que, en virtud de la trascendencia de la ciberseguridad en el ámbito nacional e internacional, es esencial establecer lazos de cooperación y alianzas estratégicas con organismos y entidades especializadas, tanto nacionales como internacionales, para fortalecer las capacidades defensivas y de respuesta del tribunal.

Por ello,

ACORDARON:

1°) Disponer la creación de la Oficina de Ciberseguridad bajo la órbita de la Dirección de Sistemas.

2°) Designar a un funcionario con categoría de Subdirector para liderar la mencionada Oficina.

3°) Aprobar la misión, funciones y objetivos de la Oficina creada por el punto 1 que, como documento anexo, forman parte integrante de la presente.

Todo lo cual dispusieron, ordenando que se comunique, publique en el Boletín Oficial y en las páginas web del Tribunal y del CIJ y se registre en el libro correspondiente, de lo que doy fe.

Firmado Digitalmente por ROSATTI Horacio Daniel

Firmado Digitalmente por ROSENKRANTZ Carlos Fernando

Firmado Digitalmente por MAQUEDA Juan Carlos

Firmado Digitalmente por FONT Damian Ignacio

ANEXO

Misión, Funciones y Objetivos de la Oficina de Ciberseguridad

I. Misión

Gestionar la seguridad cibernética de la Corte Suprema de Justicia de la Nación, asegurando la integridad, confidencialidad y disponibilidad de la información y sistemas, mediante una gestión proactiva frente a amenazas cibernéticas y promoviendo una cultura robusta de seguridad informática.

II. Funciones

1. Supervisión y Protección: Monitoreo constante de la infraestructura tecnológica para detectar, prevenir y neutralizar actividades maliciosas.
2. Gestión de Riesgos: Evaluación continua de vulnerabilidades, diseñando e implementando estrategias para su mitigación.
3. Capacitación y Concientización: Implementación de programas educativos para el personal, promoviendo prácticas seguras en el uso de tecnologías y conciencia sobre amenazas emergentes.
4. Respuesta a Incidentes: Establecimiento de un protocolo de acción rápida y coordinada ante cualquier brecha o ataque de seguridad.

5. Cumplimiento Normativo: Aseguramiento del cumplimiento de regulaciones, leyes y estándares nacionales e internacionales en materia de ciberseguridad.
6. Evaluación de Proveedores: Revisión y verificación para que los proveedores tecnológicos cumplan con los estándares de seguridad requeridos.
7. Normativas Internas: Creación, revisión y actualización de políticas y requisitos internos de seguridad informática.

III. Objetivos

1. Prevención: Desarrollo e implementación de estrategias proactivas para prevenir ataques y brechas de seguridad.
2. Formación Continua: Establecimiento de un programa de capacitación en ciberseguridad para mantener al personal al día con las mejores prácticas y tendencias.
3. Adherencia a Normativas: Asegurar que todas las operaciones y sistemas se alineen con las regulaciones y recomendaciones nacionales e internacionales.
4. Respuesta Eficaz: Diseñar y mantener protocolos claros y efectivos para una respuesta rápida en caso de incidentes de seguridad.

IV. Estrategias

1. Herramientas Avanzadas: Implementación de software y hardware especializado para monitoreo, detección y respuesta a amenazas.

2. Equipo Especializado: Formación de un equipo de expertos en ciberseguridad, constantemente actualizado sobre las últimas tendencias y amenazas.
3. Capacitaciones Regulares: Orientadas para todo el personal de la Corte, garantizando la conciencia y preparación frente a amenazas cibernéticas.
4. Colaboración Interdepartamental: Establecimiento de sinergias con otros departamentos internos y externos a la Corte Suprema de Justicia de la Nación para asegurar una implementación cohesiva y efectiva de las políticas y prácticas de seguridad.