MINISTERIO DE SEGURIDAD Y JUSTICIA
Ley Nº 9726

EL SENADO Y CÁMARA DE DIPUTADOS DE LA PROVINCIA DE MENDOZA,

SANCIONAN CON FUERZA DE

LEY:

CAPÍTULO I

DISPOSICIONES GENERALES

ART. 1 La presente ley establece los presupuestos mínimos que regirán el marco institucional de gobernanza, la gestión del riesgo, la ejecución operativa, la fiscalización técnica y el control de la ciberseguridad en la Provincia, asegurando la confidencialidad, integridad, disponibilidad, continuidad y resiliencia de los servicios públicos digitales, protegiendo los datos personales, resguardando la infraestructura digital crítica provincial y reduciendo el riesgo sistémico digital.

ART. 2 Las siglas, conceptos y definiciones técnicas de importancia para la implementación de esta norma, se encuentran detallados en el Anexo que forma parte de la presente ley.

CAPÍTULO II

OBLIGACIONES GENERALES Y PRINCIPIOS RECTORES

ART. 3 La política provincial de ciberseguridad se regirá por los siguientes principios:

a) Gestión basada en riesgo: las medidas de ciberseguridad deberán definirse en función de la probabilidad e impacto de los riesgos identificados.

b) Proporcionalidad: las obligaciones y medidas deberán ser proporcionales a la criticidad de los activos, servicios, datos e infraestructuras involucradas.

c) Confidencialidad, integridad, disponibilidad y trazabilidad: la gestión de ciberseguridad deberá proteger la información contra accesos no autorizados, alteraciones indebidas, destrucción, indisponibilidad o uso ilegítimo.

d) Continuidad y resiliencia: las acciones deberán orientarse a mantener la prestación de los servicios públicos digitales, incluso en condiciones degradadas, y a recuperar su funcionamiento ante incidentes.

e) Control de daños: ante incidentes de ciberseguridad deberán adoptarse medidas oportunas para evitar su propagación, escalamiento o impacto sobre otros organismos, sistemas o servicios.

f) Coordinación institucional: los organismos alcanzados deberán actuar de manera coordinada, evitando duplicidad, contradicción o interferencia de funciones.

g) Responsabilidad compartida: cada organismo será responsable de la seguridad de sus datos, activos, sistemas y servicios, dentro del marco rector establecido por la presente ley.

h) Seguridad y privacidad desde el diseño: los sistemas, plataformas, integraciones y servicios digitales deberán incorporar criterios de seguridad y protección de datos desde su diseño, desarrollo, adquisición, implementación y operación.

i) Respuesta responsable: las medidas de respuesta ante incidentes deberán orientarse exclusivamente a la prevención, contención, mitigación, recuperación y mejora continua, quedando excluidas acciones ofensivas.

j) Mejora continua: el sistema provincial de ciberseguridad deberá actualizarse periódicamente conforme a la evolución tecnológica, normativa y del entorno de amenazas.

CAPÍTULO III

AUTORIDAD DE APLICACIÓN Y GOBERNANZA ESTRATÉGICA

ART. 4 Créase el Comité de Conducción Estratégica de Ciberseguridad, en adelante CCEC, como autoridad de aplicación de la presente ley e instancia superior de gobernanza estratégica y política en materia de ciberseguridad provincial.

El CCEC tendrá carácter estratégico, normativo, de supervisión institucional y de fiscalización técnica, sin intervenir en la ejecución operativa cotidiana de las capacidades técnicas de ciberseguridad.

Sus integrantes deberán ostentar la jerarquía institucional correspondiente a las direcciones de tecnologías de los ministerios del Poder Ejecutivo o en su defecto quien sea designado por la autoridad de cada Ministerio Provincial.

La ejecución operativa de las capacidades técnicas de ciberseguridad estará a cargo de la Autoridad de Ejecución Operativa prevista en la presente ley.

ART. 5 El CCEC estará integrado por representantes designados por el Poder Ejecutivo Provincial, conforme lo establezca la reglamentación, la que establecerá los procedimientos aplicables para la toma de decisiones hacia adentro del cuerpo, y demás aspectos atinentes a su funcionamiento.

ART. 6 El CCEC designará un Coordinador General, quien tendrá a su cargo la coordinación administrativa e institucional del Comité, la convocatoria y organización de reuniones, el seguimiento de acuerdos, la articulación con la Autoridad de Ejecución Operativa, la articulación con la función técnica de fiscalización y control del CCEC y la elevación de informes de avance.

El Coordinador General no sustituirá las competencias propias del CCECC ni de la Autoridad de Ejecución Operativa.

ART. 7 El CCEC tendrá como mínimo las siguientes funciones:

a) Elaborar el Plan Provincial de Ciberseguridad que contenga la política provincial de ciberseguridad;

b) Elevar al Poder Ejecutivo el Plan Provincial de Ciberseguridad para su aprobación.

c) Dictar estándares, guías, lineamientos técnicos y requisitos mínimos obligatorios de ciberseguridad;

d) Aprobar criterios de clasificación de criticidad de activos, servicios, organismos e infraestructura digital;

e) Definir etapas y prioridades de implementación conforme al riesgo, criticidad, exposición y disponibilidad presupuestaria;

f) Supervisar estratégicamente la implementación del Plan Provincial de Ciberseguridad;

g) Ejercer la fiscalización técnica y el control de cumplimiento de la política provincial de ciberseguridad;

h) Requerir informes de cumplimiento a la Autoridad de Ejecución Operativa, a los organismos alcanzados y a los proveedores involucrados;

i) Disponer medidas de cumplimiento institucional en los casos previstos por esta ley y su reglamentación;

j) Establecer indicadores, métricas y mecanismos de evaluación de cumplimiento y madurez en ciberseguridad, a los efectos de la mejora y evaluación continua.

k) Coordinar la política de ciberseguridad con otros poderes, municipios, organismos nacionales, universidades, empresas públicas, sector privado, proveedores y organismos internacionales, en el marco de sus respectivas competencias;

l) Aprobar indicadores, métricas y criterios de seguimiento del sistema provincial de ciberseguridad;

ll) Aprobar los criterios generales de aceptación y tratamiento del riesgo residual.

m) Recepcionar vulnerabilidades reportadas por las vías establecidas.

ART. 8 El CCEC podrá convocar una mesa técnica interinstitucional de ciberseguridad como instancia consultiva, de intervención académica e intercambio técnico, en el marco de lo que disponga la reglamentación.

ART. 9 El plan provincial de ciberseguridad establecerá los estándares, guías, lineamientos técnicos y requisitos mínimos de ciberseguridad de cumplimiento obligatorio para los organismos que queden alcanzados por el mismo. Estos deberán incluir:

a) requisitos mínimos de seguridad;

b) procedimientos de gestión de incidentes;

c) criterios de clasificación de criticidad;

d) lineamientos de continuidad y recuperación;

e) controles de cumplimiento;

f) criterios de reporte;

g) requisitos aplicables a proveedores;

h) condiciones de integración segura con plataformas provinciales;

i) criterios de aceptación y tratamiento del riesgo;

j) obligaciones diferenciadas para Infraestructura Digital Crítica Provincial;

k) condiciones mínimas de operación de capacidades SOC y CSIRT.

Los estándares y lineamientos deberán actualizarse periódicamente conforme a la evolución tecnológica, normativa, del riesgo y según las recomendaciones de la autoridad de ejecución.

CAPÍTULO IV

AUTORIDAD DE EJECUCIÓN OPERATIVA

ART. 10 La fiscalización técnica y el control sobre el plan provincial de ciberseguridad deberán mantenerse funcionalmente separados de la ejecución operativa.

La reglamentación deberá establecer mecanismos que garanticen la separación funcional entre quien ejecuta la operación técnica, quien fiscaliza técnicamente y quien aprueba políticas, estándares y decisiones estratégicas.

ART. 11 El Poder Ejecutivo, a propuesta del CCEC, designará la Autoridad de Ejecución Operativa de Ciberseguridad, en adelante Autoridad de Ejecución Operativa, responsable de implementar las capacidades operativas necesarias para la ejecución del Plan Provincial de Ciberseguridad.

La Autoridad de Ejecución Operativa podrá recaer en una estructura estatal existente o en quienes el Poder Ejecutivo determine conforme al régimen jurídico vigente.

ART. 12 La ejecución operativa de las tareas técnicas de ciberseguridad, a cargo de dicha autoridad, podrá ser realizada directamente por el estado provincial, mediante servicios gestionados por prestadores especializados, mediante esquemas mixtos o prestadores privados especializados.

La elección del modelo deberá fundarse en criterios de eficiencia, especialización, criticidad, escalabilidad, disponibilidad de capacidades, continuidad operativa, protección de la información estatal y gestión del riesgo.

En todos los casos, la supervisión, validación técnica y control de la gestión de ciberseguridad serán funciones indelegables del estado provincial y se ejercerán por el CCEC conforme a la presente ley.

ART. 13 Serán funciones de la Autoridad de Ejecución Operativa:

a) Implementar las capacidades técnicas y operativas previstas en el Plan Provincial de Ciberseguridad;

b) Ejecutar o gestionar las capacidades SOC y CSIRT provinciales;

c) Colaborar en el desarrollo, revisión y actualización del Plan Provincial de Ciberseguridad;

d) Coordinar la operación técnica de monitoreo, detección, análisis, contención, mitigación, respuesta y recuperación ante incidentes;

e) Implementar herramientas, servicios, procesos y capacidades técnicas aprobadas por la Autoridad de Aplicación;

f) Colaborar con los organismos alcanzados en la implementación de estándares obligatorios;

g) Producir informes técnicos y operativos para el CCEC;

h) Mantener registros de las actuaciones operativas realizadas;

i) Coordinar con proveedores, organismos y equipos técnicos involucrados en la operación de ciberseguridad;

j) Ejecutar las medidas urgentes de contención previstas en la presente ley, en la reglamentación y en los protocolos aprobados;

k) Cumplir las instrucciones técnicas vinculantes emitidas por el CCEC o por su función técnica de fiscalización y control en materia de control, mitigación de riesgos y gestión de incidentes;

l) Garantizar la disponibilidad de información, evidencias, reportes y registros necesarios para la fiscalización técnica.

CAPÍTULO V

ALCANCE Y SUJETOS COMPRENDIDOS

ART. 14 La presente ley será de cumplimiento obligatorio, en los términos de la reglamentación, para:

a) Poder Ejecutivo;

b) Terceros que presten servicios digitales, tecnológicos, de infraestructura, software, conectividad, nube, seguridad, soporte, procesamiento o custodia de información para el Estado provincial;

c) Toda otra entidad que opere procese, custodie o integre sistemas, datos o servicios digitales del Estado provincial, conforme lo determine la reglamentación o los instrumentos contractuales respectivos.

d) Prestadores de servicios críticos esenciales.

ART. 15 Los organismos alcanzados serán responsables de cumplir lo que disponga el CCEC y el plan provincial de ciberseguridad, en los términos de la reglamentación y de proteger los datos, sistemas, servicios, activos digitales e infraestructura bajo su administración, custodia, operación o dependencia.

A tal efecto deberán:

a) Adoptar medidas permanentes de prevención, detección, reporte, contención, mitigación y recuperación;

b) Implementar los estándares mínimos obligatorios dictados por la CCEC;

c) Designar una contraparte institucional de ciberseguridad;

d) Reportar incidentes conforme a los procedimientos establecidos;

e) Gestionar sus riesgos de ciberseguridad;

f) Colaborar con el CCEC, con su función técnica de fiscalización y control y con la Autoridad de Ejecución Operativa;

g) Cumplir los planes de adecuación, remediación o mejora que correspondan;

h) Mantener registros de cumplimiento cuando corresponda;

i) Asegurar que sus contrataciones tecnológicas contemplen requisitos de ciberseguridad.

ART. 16 Los contratos con proveedores de servicios digitales o tecnológicos deberán prever la obligación de informar vulnerabilidades, incidentes, amenazas, eventos o condiciones de riesgo que puedan afectar sistemas, datos, servicios o infraestructura del Estado provincial.

Será nula toda cláusula contractual que restrinja injustificadamente la comunicación de información necesaria para prevenir, detectar, responder, mitigar o recuperarse de incidentes de ciberseguridad, siempre que dicha comunicación se realice conforme a los deberes de confidencialidad, seguridad y protección de datos aplicables.

CAPÍTULO VI

INFRAESTRUCTURA CRÍTICA ESENCIAL

ART. 17 El CCEC identificará y clasificará la infraestructura crítica esencial, entendida como aquella donde la indisponibilidad, alteración, destrucción, compromiso o uso indebido del conjunto de sistemas, plataformas, procesos, servicios digitales, integraciones, redes, datos y activos tecnológicos de servicios esenciales, pueda afectar:

a) La continuidad de servicios públicos esenciales;

b) La validez o eficacia de actos administrativos digitales;

c) La seguridad de los datos personales;

d) El funcionamiento del ecosistema digital de integrabilidad de Mendoza;

e) La identidad digital, firma electrónica y digital, notificaciones digitales o servicios ciudadanos;

f) La confianza en los servicios digitales del estado provincial;

g) La operación de áreas estratégicas de gobierno;

h) La seguridad pública, salud, hacienda, educación, justicia, y cualquier otra función crítica del estado provincial.

ART. 18 Los organismos alcanzados deberán implementar procesos de gestión de riesgos de ciberseguridad, conforme a los lineamientos que dicte el CCEC.

Dichos procesos deberán contemplar, como mínimo:

a) Identificación de activos;

b) Clasificación de criticidad;

c) Evaluación de amenazas, vulnerabilidades e impactos;

d) Definición de medidas de tratamiento;

e) Seguimiento de riesgos residuales;

f) Documentación de decisiones relevantes.

ART. 19 Los organismos responsables de infraestructura crítica esencial deberán implementar medidas reforzadas de ciberseguridad, continuidad operativa, recuperación ante desastres, reporte de incidentes, monitoreo, gestión de vulnerabilidades, control de accesos, registro de eventos y respuesta ante incidentes, conforme lo establezca el CCEC.

Deberán asimismo mantener registros de las acciones de seguridad ejecutadas, participar en revisiones periódicas, ejercicios o simulacros cuando sean requeridos y designar una contraparte institucional responsable de su coordinación con el CCEC y la Autoridad de Ejecución Operativa.

CAPÍTULO VII

GOBIERNO DE DATOS PARA LA CIBERSEGURIDAD

ART. 20 Los sujetos alcanzados por la presente ley deberán implementar un régimen de gobierno de datos como parte integrante de su gestión de ciberseguridad, y adoptar las normas del plan de ciberseguridad en tal sentido, orientado a preservar la confidencialidad, integridad, disponibilidad, trazabilidad, autenticidad, calidad, legalidad y uso legítimo de los datos bajo su responsabilidad.

ART. 21 El régimen de gobierno de datos comprenderá la protección de datos durante todo su ciclo de vida, incluyendo creación, carga, modificación, consulta, intercambio, exportación, conservación, archivo y eliminación segura.

Incluirá como mínimo, la creación, recolección, carga, validación, modificación, consulta, transmisión, intercambio, exportación, conservación, respaldo, archivo y eliminación segura de los datos, cualquiera sea el soporte, sistema, infraestructura, plataforma o servicio tecnológico utilizado, incluyendo servicios provistos por terceros o en entornos de computación en la nube.

ART. 22 Todo acceso, intercambio, transferencia, descarga o exportación de datos deberá responder a una finalidad institucional legítima, estar autorizado conforme a perfiles definidos, quedar registrado de manera auditable y observar los principios de proporcionalidad, minimización, seguridad, confidencialidad y responsabilidad.

Los intercambios de datos entre organismos, entidades o terceros deberán instrumentarse mediante mecanismos seguros, con identificación de responsables, finalidad, categorías de datos involucradas, condiciones de uso, medidas de seguridad, plazo de conservación, régimen de trazabilidad y procedimiento de notificación ante incidentes o accesos indebidos.

ART. 23 La máxima autoridad de cada sujeto alcanzado será responsable de asegurar la implementación del régimen de gobierno de datos previsto en este capítulo, asignar recursos adecuados, aprobar políticas internas, promover la capacitación del personal y disponer revisiones periódicas de cumplimiento.

ART. 24 Las disposiciones del presente capítulo se aplicarán sin perjuicio de la normativa vigente en materia de protección de datos personales, acceso a la información pública, transparencia, archivo, confidencialidad, secreto profesional, secreto fiscal, estadístico, bancario, sanitario, defensa nacional u otros regímenes especiales.

Cuando los datos comprendidos sean datos personales, sensibles o sujetos a regímenes especiales de confidencialidad, las medidas de gobierno de datos deberán articularse con las obligaciones de licitud, finalidad, minimización, seguridad, confidencialidad, conservación limitada, derechos de los titulares y responsabilidad proactiva que resulten aplicables.

CAPÍTULO VIII

SOC, CSIRT Y GESTIÓN DE INCIDENTES

ART. 25 La Provincia contará con capacidades de Centro de Operaciones de Seguridad y Equipo de Respuesta ante Incidentes, en adelante SOC y CSIRT, bajo el modelo de ejecución que determine el Poder Ejecutivo conforme a la presente ley.

Dichas capacidades podrán ser gestionadas por la Autoridad de Ejecución Operativa, por estructuras estatales propias, o por quien designe el Estado provincial conforme al régimen jurídico aplicable.

ART. 26 Las capacidades SOC/CSIRT deberán permitir, como mínimo:

a) Monitoreo de eventos de seguridad;

b) Detección y clasificación de incidentes;

c) Análisis técnico inicial;

d) Contención y mitigación;

e) Coordinación de respuesta;

f) Registro y trazabilidad de actuaciones;

g) Elaboración de informes técnicos;

h) Apoyo a la recuperación y mejora posterior al incidente;

i) Articulación con organismos afectados;

j) Preservación inicial de evidencia digital cuando corresponda.

ART. 27 Ante incidentes críticos de ciberseguridad, la estructura operativa podrá ejecutar medidas inmediatas de contención, conforme a los protocolos aprobados.

El CCEC, a través de su función técnica de fiscalización y control, podrá instruir medidas adicionales de mitigación, segmentación, aislamiento, restricción o recuperación, las cuales serán de cumplimiento obligatorio.

Las actuaciones deberán ser registradas, fundadas técnicamente y comunicadas a la Autoridad de Aplicación conforme a los procedimientos establecidos.

ART. 28 La reglamentación establecerá un esquema escalonado de reporte de incidentes de ciberseguridad, que contemple como mínimo:

a) Alerta temprana;

b) Actualización inicial;

c) Informe final;

d) Seguimiento posterior cuando el incidente continúe activo o produzca impactos diferidos.

A tal efecto, el CCEC deberá aprobar una matriz de clasificación de severidad de incidentes, con criterios objetivos para determinar niveles de criticidad, plazos de reporte, canales de comunicación, escalamiento institucional e intervención operativa del SOC/CSIRT.

Los plazos, contenidos y canales de reporte deberán diferenciarse según criticidad, impacto, tipo de organismo afectado, afectación de infraestructura digital crítica provincial y eventual compromiso de datos personales.

ART. 29 Créase el Registro Provincial de Incidentes de Ciberseguridad, que será administrado por la Autoridad de Ejecución Operativa bajo fiscalización técnica del CCEC, conforme lo establezca la reglamentación.

El registro tendrá por finalidad:

a) Asegurar trazabilidad institucional;

b) Identificar recurrencias;

c) Mejorar la gestión del riesgo;

d) Apoyar la toma de decisiones;

e) Medir tiempos de detección, respuesta y recuperación;

f) Fortalecer la coordinación entre organismos;

g) Generar información estadística no sensible para la mejora continua.

La información contenida en dicho registro tendrá carácter reservado cuando su divulgación pudiera comprometer la seguridad de sistemas, datos, servicios o infraestructura digital del Estado provincial.

ART. 30 Toda persona humana o jurídica que detecte una vulnerabilidad de ciberseguridad en sistemas, redes, servicios del estado provincial y de organismos que adhieran a esta ley, podrá reportarla a través del canal oficial habilitado por la estructura SOC/CSIRT, conforme al programa de divulgación responsable que establezca la reglamentación.

El programa de divulgación responsable deberá contemplar, como mínimo:

a) Un canal de recepción de reportes de vulnerabilidades, de acceso público y gratuito;

b) Plazos máximos de acuse de recibo, evaluación técnica y respuesta al reportante;

c) Criterios de triaje según severidad y explotabilidad de la vulnerabilidad reportada;

d) Un compromiso de no inicio de acciones legales contra quienes reporten de buena fe, dentro del alcance autorizado por el programa y sin haber explotado, divulgado ni comercializado la vulnerabilidad;

e) Reglas de divulgación coordinada que resguarden la confidencialidad de la vulnerabilidad hasta su remediación o hasta el vencimiento de los plazos que fije la reglamentación;

f) La incorporación de los reportes recibidos al Registro Provincial de Incidentes de Ciberseguridad, cuando corresponda, a los fines de su seguimiento y mejora continua.

La Autoridad de Ejecución Operativa, bajo fiscalización técnica del CCEC, será responsable de la gestión operativa del programa de divulgación responsable y de la coordinación con los organismos afectados para la remediación de las vulnerabilidades reportadas.

ART. 31 Tendrán carácter reservado, los informes técnicos, reportes de incidentes, matrices de riesgo, planes de continuidad, planes de recuperación, planes de mitigación, configuraciones, registros técnicos, evidencias digitales, indicadores de compromiso, detalles de vulnerabilidades, arquitecturas de seguridad y demás información cuya divulgación pudiera comprometer la seguridad de los sistemas, datos, servicios o infraestructura digital del estado provincial.

ART. 32 Las personas que, por razón de sus funciones, contratación, auditoría, prestación de servicios o participación en procesos de ciberseguridad, accedan a información relacionada con el plan provincial, reservada o sensible estarán obligadas a guardar confidencialidad, incluso después de finalizada su relación laboral, contractual o funcional.

La infracción a este deber dará lugar a las responsabilidades administrativas, contractuales, civiles o penales que correspondan.

CAPÍTULO IX

CAPACITACIÓN, CULTURA Y MEJORA CONTINUA

ART. 33 El CCEC promoverá programas de capacitación, formación y concientización en ciberseguridad para agentes del estado provincial, responsables institucionales, equipos técnicos y usuarios de servicios digitales.

Los organismos deberán implementar acciones de concientización conforme a los lineamientos establecidos por la Autoridad de Aplicación.

ART. 34 En el marco de la educación y alfabetización digital, se elaborarán recomendaciones al sector privado para que este siga las guías y protocolos que establezca el CCEC en el marco de lo dispuesto en esta ley, y que contemplen:

a) Llevar adelante un tratamiento y uso responsable, seguro y cuidado de los datos y activos de la información que tenga en su poder o tratamiento, protegiendo los derechos de los titulares de los datos.

b) Implementar medidas de ciberseguridad proporcionales a la sensibilidad de los datos que gestionan.

c) En la gestión de activos de información, implementar procesos y mecanismos de seguridad, una adecuada gestión de la autenticación, autorización y control de accesos.

d) Adoptar medidas para prevenir, detectar, gestionar, reportar y resolver incidentes de seguridad o ataques que puedan afectar los activos de información.

e) Informar a los consumidores sobre políticas de protección de datos y ciberseguridad.

f) Utilizar certificados digitales y cifrado para los dispositivos de la organización.

g) Implementar mecanismos que garanticen transferencias seguras.

h) Garantizar que los productos y servicios tecnológicos ofrecidos cumplan con estándares internacionales de seguridad.

i) Reportar vulnerabilidades, incidentes de ciberseguridad que afecten los derechos de los consumidores o terceros relacionados.

j) Atender las guías y protocolos emanados del comité creado en esta ley.

ART. 35 Para la ciudadanía en general, se elaborarán campañas de concientización, información y recomendación para que sigan las guías y protocolos que establezca el CCEC en el marco de lo dispuesto en esta ley, y que contemplen:

a) Utilizar las tecnologías de información de manera segura y responsable.

b) Proteger sus credenciales y datos personales en el ciberespacio.

c) Implementar métodos de cifrado de dispositivos y utilizar certificados digitales.

d) Reportar posibles incidentes y vulnerabilidades de seguridad a las autoridades competentes.

e) Denunciar cualquier incidente, delito y/o utilización de su identidad en el ciberespacio.

CAPÍTULO X

DISPOSICIONES SANCIONATORIAS

ART. 36 El incumplimiento de lo dispuesto en esta norma y su reglamentación, de los estándares, lineamientos, instrucciones y disposiciones establecidas en el plan provincial de ciberseguridad con carácter crítico y obligatorio, supondrá sanciones a aplicarse por el CCEC.

ART. 37 Se considerarán incumplimientos graves:

a) No implementar estándares mínimos obligatorios;

b) No reportar incidentes conforme a los procedimientos establecidos;

c) Obstaculizar auditorías o requerimientos de información;

d) Entregar información técnica falsa, incompleta o manifiestamente errónea;

e) Incumplir instrucciones técnicas vinculantes durante la gestión de un incidente crítico;

f) Ocultar incidentes que puedan afectar servicios públicos, datos personales o Infraestructura Digital Crítica Provincial;

g) Incumplir medidas de mitigación o remediación dispuestas por la Autoridad de Aplicación o por la función técnica de fiscalización y control del CCEC.

ART. 38 Las sanciones serán dispuestas con criterio de razonabilidad, teniendo en cuenta la criticidad del incumplimiento, el nivel de riesgo generado y la conducta del obligado.

Serán progresivas y podrán incluir:

a) Advertencia formal;

b) Intimación de adecuación con plazo determinado;

c) Plan obligatorio de remediación;

d) Auditoría técnica extraordinaria;

e) Segmentación preventiva de servicios;

f) Restricción parcial de interconexión;

g) Suspensión de interconexión provincial en casos de riesgo sistémico;

h) Comunicación a la autoridad superior del organismo;

i) Inicio de actuaciones administrativas o contractuales, cuando corresponda.

La reglamentación determinará el procedimiento aplicable, resguardando el debido proceso administrativo y las competencias de los órganos correspondientes.

CAPÍTULO XI

DISPOSICIONES COMPLEMENTARIAS

ART. 39 Invítese a los Municipios a adherir a los principios rectores establecidos en el artículo 3 y al Plan Provincial de Ciberseguridad que se estableciere de acuerdo al artículo 9.

ART. 40 Convóquese al Poder Judicial y al Poder Legislativo a fin de que designen sus representantes al Comité enunciado en el artículo 4º, con el objeto de que contribuyan al plan de ciberseguridad y a su ejecución operativa o, en su caso, a trabajar su propio plan de conformidad con los principios de la presente ley.

ART. 41 Incorpórese como inciso t) del artículo 144 de la Ley N° 8706, de Administración Financiera, el siguiente:

“t) La adquisición, contratación, renovación, actualización, ampliación, suscripción, soporte, mantenimiento o implementación de bienes, servicios, licencias, plataformas, equipamiento, infraestructura tecnológica, soluciones de software, servicios profesionales especializados o herramientas destinadas a la ciberseguridad, seguridad digital, continuidad operativa, protección de activos de información, respuesta ante incidentes, inteligencia de amenazas, resguardo, recuperación y disponibilidad de sistemas críticos, así como aquellas tecnologías estratégicas aplicadas a la seguridad pública, será tratada como el caso del inciso a) de este artículo”

ART. 42 El Poder Ejecutivo reglamentará la presente ley dentro de los 90 días posteriores a su publicación.

ART. 43 Comuníquese al Poder Ejecutivo.

DADA EN EL RECINTO DE SESIONES DE LA HONORABLE LEGISLATURA DE LA PROVINCIA DE MENDOZA, a los dos días del mes de septiembre del año dos mil veintiséis.

SDOR. MARTÍN KERCHNER TOMBA

LIC. PABLO ANDRÉS LOMBARDI

LIC. LUCAS ADRIÁN FAURE

DRA. MARÍA CAROLINA LETTRY

NOTA: El/los Anexo/s que integra/n este Aviso Oficial se publican en el siguiente link: Anexo
o podrán ser consultados en la edición web del Boletín Oficial de la Provincia de Mendoza
www.mendoza.gob.ar/boletinoficial
Publicaciones: 1

Fecha de Publicación	Nro Boletín
14/09/2026	32676

Importe: $ 1470