PROYECTO DE LEY

El Senado y la Cámara de Diputados sancionan con fuerza de ley…

Protocolo nacional de respuesta ante incidentes cibernéticos en cuentas de redes sociales y sitios web de organismos del Estado y de funcionarios públicos

CAPÍTULO I — OBJETO, ÁMBITO Y DEFINICIONES

Artículo 1°. Objeto. La presente ley tiene por objeto crear un Protocolo Nacional de Respuesta a Incidentes Cibernéticos (PNRIC).

Este protocolo resultará aplicable a en todos los casos en que se vea comprometida la información y/o el contenido de las cuentas de redes sociales y/o sitios web oficiales, sean estos de organismos del Estado Nacional y/o de funcionarios públicos nacionales, a través de intrusiones o usos no autorizados. La aplicación del protocolo se enfocará en prevenir, detectar, contener y erradicar las intrusiones por un lado y, por el otro, en recuperar datos, información, accesos, fondos o cualquier pérdida que se hubiera producido, así como en asegurar la transparencia y la rendición de cuentas.

Artículo 2°. Ámbito de aplicación. El Protocolo Nacional de Respuesta a Incidentes Cibernéticos (PNRIC) resultará aplicable a los organismos enumerados en el artículo 8° de la ley 24.156 en aquellos casos que se vean afectados:

a) Las cuentas de redes sociales y sitios web institucionales.

b) Las cuentas oficiales personales de redes sociales de funcionarias y funcionarios públicos nacionales cuando se utilicen para comunicaciones institucionales o contengan identificación oficial.

Artículo 3°. Definiciones. A los fines de esta ley se entiende por:

a) Incidente cibernético: evento que compromete la confidencialidad, integridad, disponibilidad o control de un activo digital.

b) CERT.AR (**Computer Emergency Response Team**): Equipo de Respuesta a Incidentes de Seguridad Informática del Sector Público Nacional.

c) Notificación temprana: aviso inicial al CERT y a la plataforma afectada dentro de los plazos de esta ley.

CAPÍTULO II — GOBERNANZA, ROLES Y PREPARACIÓN

Artículo 4°. Autoridad de aplicación. Será autoridad de aplicación la Dirección Nacional de Ciberseguridad en coordinación con el CERT.AR.

Artículo 5°. Responsables institucionales. Cada organismo deberá designar un Responsable de Seguridad de la Información, un Oficial de Comunicaciones de Incidentes y un Administrador/a de cuentas con credenciales nominales.

Artículo 6°. Preparación obligatoria. En un plazo de noventa (90) días de la reglamentación, cada organismo deberá:

a) Inventariar todas las cuentas oficiales y dominios.

b) Implementar autenticación multifactorial obligatoria, preferentemente con llaves físicas y gestores de contraseñas.

c) Configurar recuperación de cuentas con correos institucionales.

d) Establecer controles de acceso y privilegios mínimos.

e) Acreditar canales de escalamiento con plataformas.

f) Aprobar un Plan de Respuesta a Incidentes alineado con estándares internacionales.

Artículo 7°. Capacitación y ejercicios. Los organismos deberán realizar capacitaciones semestrales y ejercicios anuales de simulación de incidentes.

CAPÍTULO III — DETECCIÓN Y NOTIFICACIÓN

Artículo 8°. Detección. Los organismos alcanzados por la presente ley deberán monitorear actividad inusual y conservar registros de auditoría por al menos sesenta (60) meses.

Artículo 9°. Notificación obligatoria. Ante la sospecha razonable o habiendo verificado un incidente, se deberá:

a) Dentro de un lapso no superior a una (1) hora: notificación temprana al CERT.AR.

b) Dentro de un lapso no superior a las dos (2) horas: notificación a la plataforma o proveedor afectado.

c) Dentro de un lapso no superior a las dos (3) horas: comunicación pública del incidente arbitrando los medios a los fines que dicha comunicación quede fijada al menos por el término de quince (15) días en la plataforma afectada.

CAPÍTULO IV — CONTENCIÓN, ERRADICACIÓN Y RECUPERACIÓN

Artículo 10. Contención inmediata. Las acciones de contención inmediata deben incluir rotación de credenciales, revocación de sesiones activas y solicitud de

reversión de publicaciones maliciosas y de ser necesario, el cierre de los sistemas hasta el momento en el que se resuelva la incidencia.

Artículo 11.- Erradicación y recuperación. Las acciones de erradicación y recuperación, deben incluir escaneo de malware, verificación de integridad del código y restauración desde respaldos verificados.

Artículo 12.- Preservación de evidencia. Toda evidencia digital se debe preservar con cadena de custodia a los fines de garantizar su integridad.

CAPÍTULO V — TRANSPARENCIA Y COMUNICACIÓN

Artículo 13. Comunicación pública mínima. Dentro de las tres (3) horas de detectado el inconveniente, el organismo deberá publicar una descripción del incidente, alcance preliminar, medidas adoptadas y recomendaciones a la ciudadanía.

Dicho plazo no resultará de aplicación en aquellos casos en los cuales se encontrara comprometida la defensa o la seguridad nacional.

Artículo 14.- Reportes al CERT.AR. Transcurridos a los SIETE (7) días del incidente deberá producirse un informe intermedio y, luego, a los TREINTA (30) días deberá concluirse el informe final el cual será remitido al CERT y a la Autoridad de Aplicación.

CAPÍTULO VI — MEDIDAS PREVENTIVAS ESPECÍFICAS

Artículo 15.- Medidas mínimas para cuentas en redes sociales. Las redes sociales alcanzadas por la presente ley deberán tener las siguientes medidas de seguridad:

a) Autenticadores Multifactor (MFA) con llaves físicas;
b) revisión trimestral de accesos;
c) doble aprobación para publicaciones de alto impacto;
d) uso de correos institucionales.

Artículo 16.- Medidas mínimas para sitios web y dominios. Las paginas o portales web y dominios institucionales alcanzados por la presente ley deberán tener las siguientes medidas de seguridad:

a) Extensiones de seguridad para el Sistema de Nombres de Dominio (DNSSEC);
b) Gestión segura de certificados de Seguridad en la Capa de Transporte (TLS);
c) Endurecimiento de los Sistemas de Gestión de Contenidos (CMS);
d) Backups diarios inmutables
e) Pruebas periódicas de restauración.

CAPÍTULO VII — COORDINACIÓN INTERINSTITUCIONAL Y ALCANCE FEDERAL

Artículo 17.- Coordinación. La autoridad de aplicación articulará con el Ministerio de Seguridad y los organismos que estime competentes en cada incidente, según las particularidades del caso, a los fines de su dilucidación y eventual investigación penal que pudiera corresponder.

Artículo 18.- Adhesión. Invítase a los Gobiernos Provinciales, Municipales y de la Ciudad Autónoma de Buenos Aires, a adherir al presente protocolo.

CAPÍTULO VIII — CUMPLIMIENTO, AUDITORÍA Y SANCIONES

Artículo 19. Auditoría y verificación. La autoridad de aplicación deberá verificar el cumplimiento del protocolo mediante auditorías periódicas, conforme lo establezca la reglamentación.

Artículo 20. Incumplimiento. La falta de notificación o de implementación de medidas mínimas de seguridad indicadas en los artículos 15 y 16, será considerada falta grave y hará pasible al incumplidor de las sanciones administrativas que se establezcan en la reglamentación ello sin perjuicio de las acciones penales que pudieran corresponder.

CAPÍTULO IX — DISPOSICIONES FINALES

Artículo 21. Reglamentación. El Poder Ejecutivo reglamentará la presente ley dentro de los 90 días de su promulgación.

Artículo 22. Vigencia. La ley entrará en vigencia a los sesenta (60) días de su publicación.

Artículo 23. Comuníquese al Poder Ejecutivo.

OSCAR AGOST CARREÑO

Diputado Nacional

FUNDAMENTOS

Señor Presidente:

El presente proyecto de ley busca establecer un protocolo uniforme, obligatorio, estandarizado y transparente para responder a incidentes de hackeo que comprometen la información obrante y publicada en cuentas de redes sociales y sitios web oficiales de organismos públicos y funcionarios nacionales.

La necesidad de esta norma quedó en evidencia tras el reciente hackeo de la cuenta oficial en X de la Policía Federal Argentina (PFA), donde se publicaron mensajes no autorizados que afectaron la credibilidad institucional. Este hecho reviste particular gravedad, ya que la propia fuerza encargada de tareas de ciberpatrullaje y prevención en entornos digitales no pudo garantizar la seguridad de sus canales oficiales ni explicar de manera adecuada lo sucedido.

Este vacío normativo obliga al Estado Argentino a reforzar la seguridad en la gestión de su identidad digital oficial para no comprometer la confianza de la ciudadanía, teniendo en cuenta que, si bien ya existen normas relevantes como los Requisitos Mínimos de Seguridad de la Información (DECAD N° 641/2021), el Equipo de Respuesta ante Emergencias Informáticas nacional (CERT.ar.), el Comité de Ciberseguridad y la Dirección Nacional de Ciberseguridad, ni las normas ni los organismos mencionados, han determinado un protocolo de acción coordinado legalmente obligatorio con plazos de notificación, medidas preventivas mínimas y estándares de transparencia pública.

La experiencia internacional demuestra la necesidad de un marco normativo más estricto, de este modo, la Directiva NIS2 de la Unión Europea obliga a notificar incidentes en un plazo máximo de 72 horas y a emitir informes de seguimiento, en esa misma senda, en Estados Unidos, la CISA dicta directivas obligatorias a agencias federales para remediar vulnerabilidades críticas en plazos perentorios, y publica guías de reporte y contención. Estas normas fijan estándares de responsabilidad y celeridad que fortalecen la resiliencia del sector público.

Este proyecto incorpora buenas prácticas internacionales (como las establecidas en la norma NIST SP 800-61) y las adapta al contexto argentino, fijando plazos claros, la obligatoriedad del uso de autenticación multifactor con llaves físicas, la conservación de evidencia bajo cadena de custodia y la obligación de realizar ejercicios y capacitaciones periódicas.

El objetivo es proteger a los organismos nacionales y a la ciudadanía de los daños que producen estos incidentes, que no solo afectan a la reputación institucional, sino que también pueden habilitar fraudes, estafas digitales y manipulación de información sensible.

Por todo lo expuesto, solicito a mis pares el acompañamiento del presente proyecto de ley.

OSCAR AGOST CARREÑO

Diputado Nacional