

PROYECTO DE RESOLUCIÓN

La Cámara de Diputados de la Nación Argentina

RESUELVE

ARTÍCULO 1º: DIRIGIRSE al Poder Ejecutivo Nacional, en los términos del artículo 100 inc. 11 de la Constitución Nacional, a fin de que por intermedio de los organismos competentes -en particular el Centro Nacional de Ciberseguridad, dependiente de la Secretaría de Innovación, Ciencia y Tecnología que se encuentra bajo la órbita de la Jefatura de Gabinete de Ministros- brinde a esta Cámara la información referida a la gestión de los incidentes de seguridad informática que afectan al Sector Público Nacional y a las infraestructuras críticas del país; en particular, se requiere que informe lo siguiente:

1. Si existe norma que obligue a los organismos del Sector Público Nacional, a los operadores de infraestructuras críticas o a las entidades financieras a notificar los incidentes de seguridad informática que sufran; en caso afirmativo, precise la norma, los sujetos obligados, el organismo receptor, los plazos, el contenido mínimo de la notificación y las consecuencias de su incumplimiento; en caso negativo, indique si el Poder Ejecutivo prevé establecerla.
2. Indique si existe un catálogo o registro de infraestructuras críticas, la norma que lo establece, el organismo responsable de su elaboración y actualización, y los criterios conforme a los cuales se determina qué entidades son consideradas "organizaciones críticas" a los fines de la actuación del Equipo de Respuesta ante Emergencias Informáticas Nacional ("CERT.ar").
3. Precise la distribución actual de competencias en materia de gestión de incidentes, protección de infraestructuras críticas y cibercrimen entre el Centro Nacional de Ciberseguridad y la Agencia Federal de Ciberseguridad, a partir del dictado del Decreto de Necesidad y Urgencia N° 941/2025, y los mecanismos de coordinación entre ellos.
4. Si existen convenios, protocolos o instrumentos de cualquier naturaleza para el intercambio de información sobre incidentes entre el CERT.ar y el Banco Central de la República Argentina y los reguladores sectoriales -entre ellos el ENRE, el ENARGAS, el ENACOM y la ARN-; en caso afirmativo, remita copia e informe si los incidentes notificados a dichos organismos se integran a los registros del CERT.ar.
5. Describa la metodología aplicada para el relevamiento, registro, validación y clasificación de incidentes, con indicación de las fuentes de información utilizadas, la taxonomía empleada y los umbrales que definen cada nivel de severidad.
6. Informe, para el período de 2025 a la fecha, la cantidad de incidentes cerrados y en trámite, los tiempos máximos de gestión definidos para cada nivel de severidad y el tiempo promedio efectivo de contención y cierre.

7. Si los procedimientos vigentes exigen, antes de dar por cerrado un incidente de intrusión o de compromiso de cuenta, un análisis forense que verifique la erradicación del acceso y la ausencia de mecanismos de persistencia; indique en cuántos casos se realizó durante el período que va del 2025 a la fecha.
8. Informe, para el mismo período, la cantidad de incidentes ocurridos en organismos del Sector Público Nacional en los que se accedió, reveló, modificó u obtuvo sin autorización datos personales, con indicación de las categorías de datos comprometidos -en particular datos sensibles y biométricos- y de la cantidad estimada de titulares afectados.
9. Precise si en esos casos se notificó a la Agencia de Acceso a la Información Pública AAIP y a los titulares de los datos, considerando que el artículo 7.2 del Convenio 108+, aprobado por Ley N° 27.699, obliga al responsable a notificar sin demora a la autoridad de control las violaciones de seguridad que puedan afectar gravemente los derechos de los titulares; indique en cuántos casos se efectuó cada notificación.
10. Informe la cantidad de incidentes que dieron lugar a denuncia penal o a comunicación al Ministerio Público Fiscal, y si se instruyeron actuaciones administrativas para determinar responsabilidades, considerando el deber de denunciar que el ordenamiento procesal impone a los funcionarios públicos.
11. Indique las conclusiones alcanzadas respecto de las causas raíz y los vectores de ingreso predominantes y las medidas de seguridad recomendadas y efectivamente implementadas en consecuencia.

La información requerida podrá brindarse en forma agregada, sin individualizar entidades afectadas, vulnerabilidades ni causas judiciales en trámite.

ARTÍCULO 2°: De forma.

Juan Fernando Brügge
Diputado Nacional

FUNDAMENTOS

Señor Presidente:

El presente proyecto tiene por objeto conocer cómo gestiona el Estado nacional los incidentes de seguridad informática que afectan a sus organismos y a las infraestructuras críticas del país: quién está obligado a informarlos, quién es competente para intervenir, cómo se registran, qué ocurre una vez detectados y qué se hace cuando en ellos se comprometen datos personales de los ciudadanos.

El último informe anual del Equipo de Respuesta ante Emergencias Informáticas Nacional (CERT.ar), correspondiente al año 2025, registró quinientos veinte (520) incidentes en el Sector Público Nacional y en organizaciones críticas, un diecinueve por ciento (19 %) más que el año anterior, y clasificó más del noventa y dos por ciento (92 %) de ellos como de severidad alta o crítica. En los organismos del Estado, el compromiso de cuentas -esto es, el ingreso con credenciales legítimas de agentes públicos- se convirtió en la principal amenaza, y el propio organismo advierte que los atacantes dedican cada vez más recursos a permanecer dentro de las redes. En el sector financiero, los incidentes registrados crecieron un ciento setenta por ciento (170 %).

Ese informe, sin embargo, da cuenta sólo de lo que llegó a conocimiento del CERT.ar, no de lo que efectivamente ocurrió. No explica si alguien está obligado a notificar ni con qué criterios se releva, valida y clasifica la información; no dice cuántos incidentes fueron resueltos ni si se verificó que el intruso -si este fuera el caso- fue efectivamente expulsado; no dedica una sola línea a los datos personales comprometidos, ni informa si alguno de esos hechos derivó en una denuncia penal. Como advirtió recientemente Germán Luis Kammerath en su nota "¿Quién le pondrá el cascabel al gato del cibercrimen?", los casos conocidos constituyen el piso del problema y no su verdadera dimensión.

A esa falta de información se suma una incertidumbre institucional. La Segunda Estrategia Nacional de Ciberseguridad, aprobada en 2023, incorporó la protección de las infraestructuras

críticas entre sus objetivos; el Decreto de Necesidad y Urgencia N.º 941/2025 asignó competencias en materia de cibercrimen e infraestructuras críticas a la Agencia Federal de Ciberseguridad; y la gestión de incidentes continúa a cargo del CERT.ar, en el ámbito del Centro Nacional de Ciberseguridad. Intervienen, además, el Banco Central y los reguladores sectoriales, cada uno con sus propias exigencias.

La cuestión, por otra parte, no es sólo técnica: es de derechos. Una contraseña puede cambiarse y una tarjeta puede bloquearse, pero un número de documento, una historia clínica o un dato biométrico no se reemplazan. Cuando esos datos obran en poder del Estado y resultan comprometidos, sus titulares tienen derecho a saberlo. El Convenio 108+, aprobado mediante la Ley N° 27.699, obliga al responsable a notificar sin demora a la autoridad de control las violaciones de seguridad que puedan afectar gravemente los derechos de los titulares. Interesa saber, por eso, si esa obligación se está cumpliendo.

La información requerida en este pedido puede brindarse en forma agregada, del mismo modo en que el CERT.ar ya publica sus estadísticas anuales. Y si la respuesta fuera que parte de esa información no se releva, ese dato será, en sí mismo, el mejor fundamento para que legislemos en la materia.

Creo que es clave para la seguridad digital de nuestro país desarrollar aptitudes que permitan detectar, contener, investigar y aprender de cada incidente, pero también sabemos las limitaciones existentes. Entonces, para eso, primero hay que saber.

Es nuestro deber constitucional ejercer el control sobre la gestión del Poder Ejecutivo y velar por la protección de los datos personales de los argentinos y las argentinas, conforme lo consagra el artículo 43 de la Constitución Nacional.

Por todo ello, solicito a mis pares el acompañamiento de este proyecto de resolución con su debida aprobación.

Juan Fernando Brügge
Diputado Nacional