

ASAMBLEA LEGISLATIVA DE LA REPÚBLICA DE COSTA RICA

PROYECTO DE LEY

**REFORMA A LOS ARTÍCULOS 10, 28, 30 Y 31, Y ADICIÓN DEL ARTÍCULO 10
BIS A LA LEY DE PROTECCIÓN DE LA PERSONA FRENTE AL
TRATAMIENTO DE SUS DATOS PERSONALES, LEY N.º 8968 DEL 07 DE
JULIO DEL 2011 Y SUS REFORMAS.**

**LEY PARA PROTEGER A LAS PERSONAS FRENTE A LA FILTRACIÓN DE
SUS DATOS**

**DIPUTADA
SIGRID SEGURA ARTAVIA,
Y OTROS SEÑORAS DIPUTADAS Y SEÑORES DIPUTADOS**

EXPEDIENTE N.º 25.826

PROYECTO DE LEY

REFORMA A LOS ARTÍCULOS 10, 28, 30 Y 31, Y ADICIÓN DEL ARTÍCULO 10 BIS A LA LEY DE PROTECCIÓN DE LA PERSONA FRENTE AL TRATAMIENTO DE SUS DATOS PERSONALES, LEY N.º 8968 DEL 07 DE JULIO DEL 2011 Y SUS REFORMAS.

LEY PARA PROTEGER A LAS PERSONAS FRENTE A LA FILTRACIÓN DE SUS DATOS

ASAMBLEA LEGISLATIVA:

El presente proyecto de ley tiene por objeto proteger de manera integral el derecho fundamental a la intimidad y la autodeterminación informativa de la ciudadanía frente a la creciente crisis de ciberseguridad que amenaza al país, transformando el deber estatal de custodia de la información ciudadana sensible de una pauta programática a una exigencia técnica y jurídica ineludible; para ello, se establece un estándar obligatorio de protección de datos y se instaure un régimen efectivo de transparencia, notificación perentoria y rendición de cuentas que ponga fin a la impunidad ante la exposición o negligencia en el manejo de los registros de datos los habitantes.

Sobre la Crisis Creciente de Ciberseguridad en Costa Rica y las Brechas en la Dark Web

La seguridad de los sistemas y de los datos personales que resguarda el Estado y la industria se ha debilitado con el tiempo. Lo que antes parecían problemas aislados hoy representa un riesgo constante para el país. Esta situación se hizo más evidente en 2022, cuando el grupo delictivo internacional Conti atacó sistemas informáticos importantes del Ministerio de Hacienda y de la Caja Costarricense de Seguro Social (CCSS). El ataque paralizó los sistemas de aduanas y afectó la recaudación y la facturación del Estado. Además, dejó en evidencia que muchas instituciones usaban sistemas antiguos, tenían redes poco protegidas y no contaban

con suficientes medidas de cifrado para evitar que la información pudiera leerse después de un acceso no autorizado.

Esta vulnerabilidad adquirió una dimensión crítica con la detección en foros clandestinos de la *dark web* de una publicación consistente en la comercialización masiva de más de 400 millones de registros de habitantes de Costa Rica por una cifra irrisoria de 2.500 dólares. Las pericias y muestras verificadas por el Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones (MICITT) corroboraron que una fracción sustancial de los archivos expuestos constituía información real, actualizada y verosímil de ciudadanos costarricenses. La fuga comprendió datos altamente sensibles y de acceso restringido, abarcando remuneraciones salariales exactas, números de teléfono privados, correos electrónicos, domicilios residenciales e imágenes fotográficas idénticas a las registradas en el padrón electoral oficial custodiado por el Tribunal Supremo de Elecciones (TSE).

Esta filtración no se debió a un único ataque externo. También combinó accesos no autorizados a bases de datos de empresas (como Cero Riesgo) con filtraciones anteriores de instituciones públicas. Entre ellas se encuentra la extracción, años atrás, de padrones con fotografías por exfuncionarios del TSE. Esa información circuló sin protección adecuada en mercados informales. La difusión descontrolada de estos datos llevó a la Agencia de Protección de Datos de los Habitantes (PROD HAB) a iniciar una investigación de oficio, bajo el expediente N.º 425-09-2026, y motivó denuncias ante el Ministerio Público. Las autoridades advirtieron riesgos inmediatos de suplantación de identidad, estafas bancarias, extorsiones y engaños masivos dirigidos a la población.

A continuación, se detallan los principales incidentes de infiltración de datos registrados en Costa Rica:

Tabla 1: Principales incidentes de filtración de datos en Costa Rica

Incidente	Actores Involucrados	Tipología de Datos Afectados	Vector de Falla Técnica	Consecuencias Jurídicas e Institucionales
Ciberataque Masivo Conti (2022)	Grupo Conti; Ministerio de Hacienda, CCSS, MICITT.	Datos tributarios, planillas estatales, propiedad intelectual, expedientes clínicos.	Brechas perimetrales, ausencia de segmentación y almacenamiento o en claro.	Declaratoria de emergencia nacional; contingencia en aduanas y pagos de salarios.
Fuga Histórica del Padrón (Divulgada en 2026)	Exfuncionario del TSE; intermediarios y burós comerciales.	Padrón registro con fotografía oficial de cédula de identidad.	Exfiltración interna mediante credenciales legítimas sin cifrado de base.	Despido, denuncia ante el Ministerio Público e investigaciones periciales.
Filtración Masiva en la <i>Dark Web</i> (Septiembre 2026)	Ciberactor «Jarol1488»; burós de crédito privados y registros públicos.	Más de 400 millones de registros: salarios, fotos, finanzas y domicilios.	Exfiltración de repositorios consolidados carentes de salvaguardas criptográficas.	Expediente PRODHAB 425-09-2026, causas penales y riesgo sistémico de fraude.

Fuente: elaboración propia.

La extracción y exposición repetida de estos datos demuestra que los controles y defensas informáticas no son suficientes si la información no está cifrada. Cuando se guardan datos sin protección, basta con superar una barrera de seguridad o con

que una persona autorizada haga un uso indebido de su acceso para poner en riesgo la privacidad de la ciudadanía. En cambio, el uso obligatorio de un cifrado sólido hace que los datos robados no puedan ser leídos por quienes no tengan la clave correspondiente, lo que mitiga considerablemente el daño y reduce su valor para la venta ilegal o la extorsión.

Limitaciones Legales y Prácticas de la Ley N.º 8968

La Ley N.º 8968, Ley de Protección de la Persona frente al Tratamiento de sus Datos Personales, fue creada en 2011 con reglas generales y pocas herramientas para responder a los ataques informáticos actuales y a las fallas de seguridad en sistemas conectados. Después de más de una década de aplicación, la ley todavía presenta vacíos que dificultan una supervisión efectiva y permiten que se evite asumir responsabilidad ante filtraciones de datos de gran magnitud.

El artículo 10 de la Ley N.º 8968 obliga a la persona responsable de una base de datos a tomar medidas técnicas y de organización para proteger la información. Sin embargo, la ley no establece requisitos mínimos de seguridad y deja esos detalles al reglamento. Un ejemplo de esos requisitos mínimos de seguridad no exigidos de forma expresa por nuestra legislación y que constituye una herramienta esencial para la protección de datos es el cifrado.

Asimismo, la ley no obliga a informar de inmediato los incidentes o fallas de seguridad. Esto permite que entidades públicas y privadas oculten o retrasen la comunicación de una filtración o vulneración de sus sistemas o bases de datos, e impide que las autoridades o personas afectadas tomen medidas a tiempo para protegerse de posibles fraudes.

Fundamentación Jurídica de la Reforma

El Derecho a la Autodeterminación Informativa como Derivación del Artículo 24 Constitucional

El artículo 24 de la Constitución Política de Costa Rica protege la privacidad de los documentos y las comunicaciones, como parte del derecho a la intimidad y a la dignidad humana. La Sala Constitucional, mediante las sentencias N.º 2000-02381, N.º 2011-005833 y N.º 2020-008450, esta última relacionada con la Unidad Presidencial de Análisis de Datos (UPAD), reconoció la autodeterminación informativa como un derecho fundamental independiente. Este derecho no se limita a permitir que una persona autorice la recolección de sus datos, sino que también le permite conocer cómo se usan, solicitar su corrección y exigir que se mantengan seguros y confidenciales.

Al cumplir sus funciones, el Estado reúne y almacena grandes cantidades de datos personales porque así lo exige la ley. La ciudadanía no puede negarse a figurar en registros tributarios, electorales o de salud. Por esa razón, el Estado tiene un deber especial de proteger esa información. Si no adopta medidas adecuadas de seguridad, podría vulnerar directamente el derecho a la intimidad reconocido por la Constitución Política y dejar a las personas expuestas a redes delictivas que venden datos en la dark web. Por tanto, proteger la información no es una decisión técnica opcional, sino una obligación constitucional.

De igual manera, la industria comparte una responsabilidad ineludible en este esquema de protección. La experiencia reciente demuestra que las filtraciones masivas rara vez provienen de un único frente; proliferan cuando fallas en empresas (como burós comerciales o plataformas financieras) se cruzan con datos del sector público, permitiendo la reconstrucción integral de la identidad de las personas para fines extorsivos o fraudulentos. La debida diligencia y las salvaguardas criptográficas deben exigirse con idéntica rigurosidad en el ámbito empresarial para cerrar definitivamente las puertas al tráfico ilícito de información

El Cifrado Como Garantía Constitucional del Deber de Custodia de Datos Personales

El principio de proporcionalidad y el estándar de debida diligencia exigen que los responsables de bases de datos adopten medidas idóneas, necesarias y suficientes

para resguardar la información de los habitantes. Si bien el Estado recopila estos datos en el ejercicio de sus potestades de imperio y las empresas lo hacen al amparo de actividades comerciales, contractuales o financieras, ni la ley ni el consentimiento informado pueden convertirse en una vía libre para exponer la vida privada. En el entorno tecnológico contemporáneo, el cifrado sólido es la salvaguarda primordial para neutralizar cualquier acceso ilegítimo, impidiendo que terceros descifren o comercialicen la información sustraída.

Establecer por mandato legal el cifrado obligatorio para las bases de datos administradas tanto en el sector público como en el privado no vulnera el principio de reserva de ley ni restringe la adaptación ante el avance tecnológico. La ley consagra el requisito sustantivo mínimo e inderogable: ninguna entidad u organismo custodio podrá almacenar datos sensibles o de acceso restringido en texto plano o desprotegido. En paralelo, las especificaciones técnicas dinámicas, tales como familias de algoritmos robustos y pautas de gobernanza de llaves criptográficas, quedarán bajo la potestad rectora del MICITT a través de normas técnicas periódicas, garantizando una respuesta ágil frente a la constante evolución de las ciberamenazas.

Régimen Sancionatorio, Culpabilidad y Responsabilidad del Servidor Público

Un régimen sancionatorio frente a vulneraciones de seguridad y filtraciones de datos personales debe observar con estricta rigurosidad los principios constitucionales de legalidad, tipicidad y debido proceso, consagrados en los artículos 39 y 129 de la Constitución Política. La jurisprudencia vinculante de la Sala Constitucional ha reiterado que el *ius puniendi* administrativo (es decir, la potestad soberana del Estado para castigar e imponer sanciones en la vía administrativa) está sometido a las mismas garantías materiales que rigen en materia penal: las infracciones deben encontrarse descritas de manera clara, precisa e inequívoca en la norma legal, proscribiendo la analogía en perjuicio del administrado y rechazando cualquier manifestación de responsabilidad objetiva. Ninguna persona física o jurídica puede ser sancionada por el mero acaecimiento de un resultado lesivo si no media dolo o

culpa grave debidamente comprobada en el procedimiento administrativo correspondiente.

En congruencia con estos límites constitucionales, la reforma que se plantea no penaliza el hecho fortuito o inevitable de que una entidad sea blanco de un ciberataque, reconociendo que en el entorno tecnológico actual la seguridad absoluta no existe. La tipicidad se circunscribe a conductas activas u omisivas que quebranten de forma culpable los estándares de debida diligencia técnica y legal:

- Inobservancia del estándar de cifrado preceptivo: Se sanciona mantener, procesar o custodiar en el sector público datos sensibles o de acceso restringido en texto claro o mediante algoritmos técnicamente superados, infringiendo el mandato legal del artículo 10 (artículo 31, inciso f).
- Culpabilidad calificada en brechas y filtraciones: Se tipifica provocar, facilitar, permitir o encubrir la sustracción, filtración masiva o tráfico ilícito de datos personales únicamente cuando medie dolo o negligencia inexcusable en las labores de mantenimiento y vigilancia informática (artículo 31, inciso g).
- Incumplimiento del régimen de notificación y transparencia: Se sanciona el retardo injustificado o la omisión deliberada de informar a la PRODHAB y a los titulares afectados sobre incidentes de seguridad conforme a los plazos y términos previstos en el artículo 10 bis, distinguiendo con claridad las faltas graves de las gravísimas según el nivel de riesgo y la naturaleza de los registros comprometidos (artículo 30, incisos h e i; artículo 31, inciso h).

Asimismo, la modificación al artículo 28 introduce un marco sancionatorio graduado y proporcional, que dota al ordenamiento de un verdadero efecto disuasorio frente a la negligencia institucional en cuanto a la seguridad y resguardo efectivo de los datos mediante el aumento de las multas para las faltas gravísimas a un rango de 30 a 50 salarios base del cargo de auxiliar judicial se asegura que las consecuencias jurídicas guarden estricta consonancia con el daño potencial ocasionado a los derechos fundamentales de los titulares de los datos.

Modificaciones Sugeridas a la Ley N.º 8968

Para fortalecer la protección de datos en Costa Rica de forma integral, se propone reformar los artículos 10, 28, 30 y 31 de la Ley N.º 8968, además de añadir los artículos 10 bis y 10 ter. Modificar un solo numeral resultaría insuficiente, debido a que la obligación de cifrar los datos debe complementarse necesariamente con un procedimiento riguroso para la notificación oportuna de incidentes de seguridad y con un régimen sancionatorio provisto de un verdadero efecto disuasorio.

En primer término, el artículo 10 se reforma para transformar una pauta hasta ahora meramente programática en un mandato preceptivo, vinculante e indelegable, obligando a implementar salvaguardas de cifrado de extremo a extremo sobre todos los datos sensibles y de acceso restringido bajo su custodia. Dicho estándar abarca tanto los datos en reposo, almacenados en servidores físicos o virtuales, discos, respaldos y terminales periféricos, como los datos en tránsito que atraviesen redes internas o externas de telecomunicaciones. Para asegurar su actualización continua, se encomienda al Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones (MICITT) emitir y revisar el catálogo de estándares mínimos y protocolos de ciclo de vida de llaves criptográficas.

En estrecha coherencia con lo anterior, la incorporación del artículo 10 bis consagra una regla sustantiva de clausura: la prohibición absoluta e inderogable de archivar o mantener repositorios de datos personales sensibles en formatos no cifrados o empleando algoritmos técnicamente obsoletos. Esta disposición elimina cualquier margen de discrecionalidad u omisión operativa en el tratamiento de la información, blindando la privacidad de los habitantes al tipificar como una falta intolerable el almacenamiento en texto claro, tanto en el sector público como en el privado.

De manera complementaria, el nuevo artículo 10 ter introduce la obligación ineludible de notificar formalmente a la Agencia de Protección de datos de los Habitantes (PROD HAB) sobre cualquier incidente o vulneración que comprometa la confidencialidad, integridad o disponibilidad de datos personales en un plazo máximo e improrrogable de setenta y dos horas naturales, contadas a partir del

conocimiento del hecho, imponiendo además al encargado de tratamiento el deber de alertar al responsable en un lapso no mayor a veinticuatro horas. Esta notificación a PRODHAB debe detallar las características del incidente, el volumen aproximado de personas afectadas, las consecuencias previsibles, el estado criptográfico de los registros y las medidas de contención ejecutadas.

En materia sancionatoria, la iniciativa actualiza el artículo 28 para graduar las consecuencias económicas conforme a la gravedad de los riesgos informáticos actuales, elevando el reproche para las faltas gravísimas a una multa de entre treinta y cincuenta salarios base del cargo de auxiliar judicial, con lo cual se evita que las sanciones continúen siendo asumidas como un costo operativo menor por parte de las entidades infractoras.

En estrecha concordancia con lo anterior, los artículos 30 y 31 delimitan las infracciones según su grado de lesividad. El artículo 30 incorpora como faltas graves omitir medidas técnicas mínimas en bases de datos comunes, retardar injustificadamente la notificación formal de brechas cuando no exista un peligro inminente y masivo, e infringir los lineamientos técnicos del MICITT en la gestión o almacenamiento de llaves criptográficas cuando no se haya consumado una fuga de información. Por su parte, el artículo 31 califica como faltas gravísimas almacenar o custodiar en el sector público datos sensibles o de acceso restringido sin las salvaguardas de cifrado exigidas por ley, provocar, facilitar, permitir o encubrir por dolo o negligencia inexcusable la filtración masiva o comercio ilícito de información personal, y ocultar deliberadamente o consignar datos falsos ante la autoridad sobre un incidente de seguridad.

Finalmente, las disposiciones transitorias trazan una ruta progresiva y jurídicamente ordenada para la entrada en vigor del nuevo régimen, concediendo al MICITT un plazo prudencial a partir de la publicación de la ley para oficializar la reglamentación de los estándares criptográficos obligatorios, y otorgando a toda la Administración Pública un plazo prudencial para culminar la adecuación técnica integral de sus infraestructuras, servidores, canales de transmisión y dispositivos periféricos. En paralelo y de forma inmediata, se ordena a los jerarcas institucionales realizar las

previsiones administrativas y las adecuaciones internas en sus planes operativos para garantizar el acatamiento pleno de esta reforma. En igual sentido y atendiendo a criterios de razonabilidad y seguridad jurídica, se contempla un plazo prudencial para que los actores del sector privado que custodien datos sensibles formulen y ejecuten un plan de actualización técnica que adecue sus métodos de almacenamiento a las exigencias criptográficas de esta ley. Con ello, Costa Rica neutraliza la vulnerabilidad originada en el almacenamiento de datos no cifrados y asegura que, ante cualquier eventual intrusión informática, los datos sustraídos resulten técnica e irreversiblemente inaccesibles para fines ilícitos o extorsivos.

Por lo anterior, se somete a consideración de las diputadas y IOs diputados el siguiente proyecto de ley:

LA ASAMBLEA LEGISLATIVA DE LA REPÚBLICA DE COSTA RICA

DECRETA:

REFORMA A LOS ARTÍCULOS 10, 28, 30 Y 31, Y ADICIÓN DEL ARTÍCULO 10 BIS A LA LEY DE PROTECCIÓN DE LA PERSONA FRENTE AL TRATAMIENTO DE SUS DATOS PERSONALES, LEY N.º 8968 DEL 07 DE JULIO DEL 2011 Y SUS REFORMAS.

LEY PARA PROTEGER A LAS PERSONAS FRENTE A LA FILTRACIÓN DE SUS DATOS

ARTÍCULO 1.- Se reforman los artículos 10 y 28 de la Ley de Protección de la Persona frente al Tratamiento de sus Datos Personales, Ley N.º 8968 de 7 de julio de 2011 y sus reformas, para que en adelante se lean de la siguiente manera:

“ARTÍCULO 10.- Seguridad técnica y obligatoriedad de cifrado de datos.

El responsable de la base de datos deberá adoptar las medidas de índole técnica y de organización necesarias para garantizar la seguridad de los datos de carácter personal y evitar su alteración, destrucción accidental o ilícita, pérdida, tratamiento o acceso no autorizado, así como cualquier otra acción contraria a esta ley.

Dichas medidas deberán incluir, al menos, los mecanismos de seguridad física y lógica más adecuados de acuerdo con el desarrollo tecnológico actual, para garantizar la protección de la información almacenada.

No se registrarán datos personales en bases de datos que no reúnan las condiciones que garanticen plenamente su seguridad e integridad, así como la de los centros de tratamiento, equipos, sistemas y programas.

Será de acatamiento obligatorio e indelegable para organismos públicos o privados, implementar salvaguardas de cifrado de extremo

a extremo sobre todos los datos personales sensibles, datos personales de acceso restringido, datos personales de acceso irrestricto y datos referentes al comportamiento crediticio bajo su custodia. Esta exigencia criptográfica regirá de manera obligatoria tanto para los datos en reposo, almacenados en servidores centrales, infraestructuras en la nube, discos locales, cintas de respaldo y terminales periféricos, como para los datos en tránsito que crucen redes de telecomunicación internas o externas.

El Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones (MICITT), en su condición de ente rector en ciberseguridad, emitirá y actualizará anualmente, el catálogo de estándares criptográficos mínimos, familias algorítmicas reconocidas y protocolos de rotación y custodia del ciclo de vida de llaves criptográficas.

Por vía de reglamento se establecerán los requisitos y las condiciones que deban reunir las bases de datos automatizadas y manuales, y de las personas que intervengan en el acopio, almacenamiento y uso de los datos.”

“ARTÍCULO 28.- Sanciones

Si se ha incurrido en alguna de las faltas tipificadas en esta ley, se deberá imponer alguna de las siguientes sanciones, sin perjuicio de las sanciones penales correspondientes:

- a) Para las faltas leves, una multa hasta de **veinte** salarios base del cargo de auxiliar judicial I, según la Ley de Presupuesto de la República.
- b) Para las faltas graves, una multa de **veinte a cincuenta** salarios base del cargo de auxiliar judicial I, según la Ley de Presupuesto de la República.

c) Para las faltas gravísimas, una multa de **cincuenta a ochenta** salarios base del cargo de auxiliar judicial I, según la Ley de Presupuesto de la República, y la suspensión para el funcionamiento del fichero de uno a seis meses.”

Artículo 2.- Se adicionan los incisos f), g) e h) al artículo 30 y los incisos g), h) y i) al artículo 31 de la Ley de Protección de la Persona frente al Tratamiento de sus Datos Personales, Ley N.º 8968 de 7 de julio de 2011 y sus reformas, para que en adelante se lean de la siguiente manera:

“ARTÍCULO 30.- Faltas graves.

Serán consideradas faltas graves, para los efectos de esta ley:

(...)

f) Omitir la adopción de las medidas técnicas u operativas mínimas de seguridad previstas en esta ley y su reglamento, en las bases de datos que almacenen datos personales que gocen de la categoría de sensibles o datos referentes al comportamiento crediticio .

g) Retardar injustificadamente la comunicación formal y obligatoria a la Prodhav y a los titulares afectados de un incidente de seguridad, según las reglas del artículo 10 bis de esta ley, en aquellos supuestos en los que la afectación amenace de forma inminente volúmenes masivos de datos la población o datos de naturaleza biométrica o crediticia.

h) Administrar, almacenar o compartir llaves criptográficas asignadas a la protección de bases de datos en contradicción con los lineamientos técnicos fijados por el MICITT, siempre que de dicha conducta no se haya desprendido una vulneración efectiva de la confidencialidad de la información.”

“ARTÍCULO 31.- Faltas gravísimas.

Serán consideradas faltas gravísimas, para los efectos de esta ley:

[...]

g) Almacenar, procesar o custodiar datos personales sensibles o de acceso restringido omitiendo la aplicación de los estándares de cifrado establecidos en el artículo 10 de la presente ley.

h) Provocar, facilitar, permitir o encubrir, por dolo o negligencia inexcusable en el mantenimiento y vigilancia de los sistemas informáticos, la sustracción, filtración, exfiltración, fuga, robo, comercialización ilícita o vulneración de cualquier tipo de datos personales resguardados en bases de datos públicas o privadas.

i) Ocultar, dilatar deliberadamente o consignar información falsa o inexacta respecto de una brecha de seguridad que comprometa la confidencialidad de datos sensibles o datos referentes al comportamiento crediticio.”

ARTÍCULO 4.- Se adicionan los artículos 10 bis y 10 ter a la Ley de Protección de la Persona frente al Tratamiento de sus Datos Personales, Ley N.º 8968 de 7 de julio de 2011 y sus reformas, cuyo texto se leerá de la siguiente manera:

“ARTÍCULO 10 bis.- Prohibición de almacenar datos no cifrados

Queda absolutamente prohibido mantener o archivar repositorios de datos personales sensibles en formatos no cifrados o utilizando algoritmos calificados internacionalmente como obsoletos o vulnerables.”

“ARTÍCULO 10 ter.- Obligación de notificación de brechas de seguridad

Toda persona responsable de bases de datos públicas o privadas que confirme o tenga indicios fundados de una brecha o vulneración en la seguridad de sus sistemas que comprometa la confidencialidad, integridad o disponibilidad de datos personales, deberá notificarlo a la Prodhav sin dilación indebida y en un plazo máximo de setenta y dos horas naturales, contadas a partir de que tenga conocimiento del incidente.

Cuando el tratamiento sea efectuado por personas físicas o jurídicas externas a los organismos públicos o privados responsables de las bases de datos, éstas tendrán la obligación ineludible de comunicar el incidente al responsable de la base de datos de forma inmediata y, a más tardar, dentro de las veinticuatro horas siguientes a su detección.

La notificación formal a la Prodhav contendrá, como mínimo:

- a) La naturaleza y características del incidente de seguridad.
- b) Las categorías y el número aproximado de titulares y registros potencialmente afectados.
- c) Las posibles consecuencias y perjuicios que puedan derivarse para los derechos de los titulares.
- d) El estado de cifrado o las medidas técnicas de protección bajo las cuales se encontraban los datos comprometidos.
- e) Las medidas de contención, mitigación y correctivas temporales implementadas de forma inmediata o previstas para subsanar el incidente.

Si no fuera factible suministrar la totalidad de la información requerida dentro del plazo de setenta y dos horas, el responsable presentará una

comunicación preliminar y completará la información requerida en fases sucesivas sin dilación indebida, justificando los motivos técnicos de la demora.

Cuando la brecha de seguridad suponga un alto riesgo para los derechos e intereses de los titulares, particularmente si compromete datos sensibles, datos de acceso restringido, información financiera, credenciales de autenticación o datos susceptibles de propiciar fraudes o suplantación de identidad, el responsable deberá comunicar el suceso de manera expedita y directa a las personas afectadas, mediante los contactos o medios conocidos o indicados previamente. Dicha comunicación se emitirá en un lenguaje claro y comprensible, con recomendaciones concretas de seguridad y las medidas puestas a su disposición para mitigar eventuales perjuicios.”

DISPOSICIONES TRANSITORIAS

TRANSITORIO I.- El MICITT reglamentará los estándares criptográficos obligatorios en un plazo de seis meses a partir de la publicación en el diario oficial La Gaceta de la presente ley.

TRANSITORIO II.- Toda la Administración Pública, central y descentralizada, territorial e institucional, así como las empresas públicas, sujetos a las disposiciones de esta ley gozarán de un plazo de dieciocho meses a partir de la publicación en el diario oficial La Gaceta de la presente ley, para completar la adecuación criptográfica integral de sus bases de datos en reposo, infraestructuras en servidores físicos o en la nube, canales de transmisión de datos y dispositivos periféricos.

TRANSITORIO III.- Los jefes de las dependencias públicas deberán adoptar las provisiones administrativas y los ajustes internos presupuestarios indispensables en sus planes operativos inmediatos, garantizando la suficiencia de recursos

tecnológicos y de contratación pública orientados a cumplir las exigencias de cifrado fijadas en el artículo 10 de esta ley.

TRANSITORIO IV.- Las personas físicas o jurídicas de carácter privado que, a la entrada en vigencia de la presente ley, administren bases de datos con información personal sensible o datos referentes al comportamiento crediticio, contarán con un plazo de dos años para elaborar y ejecutar un plan de actualización técnica de sus métodos de almacenamiento que garantice el cumplimiento de las exigencias de cifrado fijadas en el artículo 10 de esta ley.

Rige a partir de su publicación.

Sigrid Segura Artavia
