DEPARTAMENTO DE

AGRICULTURA

GOBIERNO DE PUERTO RICO

PROTOCOLO SOBRE NOTIFICACIÓN AL CIUDADANO POR INCIDENTE DE COMPROMISO DE DATOS PERSONALES

PROTOCOLO SOBRE INFORMACIÓN AL CIUDADANO SOBRE SEGURIDAD DE BANCOS DE INFORMACIÓN

I. DISPOSICIONES GENERALES

A. AUTORIDAD LEGAL

Este Protocolo se promulga de conformidad con los poderes conferidos al Secretario del Departamento de Agricultura (DA) y sus agencias adscritas, a saber: la Administración para el Desarrollo de Empresas Agropecuarias (ADEA), la Autoridad de Tierras de Puerto Rico (ATPR), el Fondo de Innovación para el Desarrollo Agrícola (FIDA) y la Corporación de Seguros Agrícolas (CSA), por virtud del Artículo IV, Sección 6 de la Constitución de Estado Libre Asociado de Puerto Rico y se rige por el Plan de Reorganización Núm. 4 de 29 de julio de 2010, conocido como "Plan de Reorganización del Departamento de Agricultura de 2010"; las Leyes Núm. 111 de 7 de septiembre de 2005, Núm. 134-1977, Núm. 40-2024, la Orden Ejecutiva 14028 de los Estados Unidos, Estándares NIST SP 800-61, y SP 800-171, y reglamentos aplicables emitidos por el Departamento de Asuntos del Consumidor (DACO) y la Oficina del Procurador del Ciudadano, según enmendadas respectivamente.

B. PROPÓSITO

Este protocolo tiene el propósito de establecer un procedimiento que garantice la notificación oportuna los ciudadanos afectados de cualquier violación de la seguridad del sistema, notificación obligatoria a DACO y a la Oficina del Procurador del Ciudadano, la protección efectiva de la información personal y el cumplimiento con las normas de ciberseguridad vigentes. Pretende, además, establecer los derechos y responsabilidades de toda entidad propietaria o custodia de bancos de información, que incluyan información personal de los ciudadanos residentes en Puerto Rico, al igual que las responsabilidades y obligaciones de toda entidad que provea acceso a tales bancos de información. Por otra parte, define términos, y establece los procedimientos y responsabilidades para notificar a ciudadanos cuya información personal pueda haberse visto comprometida por incidentes de seguridad, asegurando el cumplimiento legal y la protección de la privacidad.

C. INTERPRETACIÓN

Este protocolo deberá interpretarse liberalmente a favor de los ciudadanos, priorizando la transparencia, la pronta respuesta y la protección de datos, conforme y en ánimo de cumplir con los mandatos de las Leyes Núm. 111, y Núm. 134, según enmendadas respectivamente. En caso de discrepancias entre el texto original en español y su traducción al inglés, prevalecerá el texto en español. Las palabras y frases usadas en este protocolo se interpretarán según el contexto en que sean usadas y tendrán el significado sancionado por el uso común y corriente. En los casos aplicables, las palabras utilizadas en el tiempo presente incluyen también el futuro; las usadas en el género masculino incluyen el femenino; el singular incluye el plural y el plural incluye el singular.

II. DEFINICIONES

A. Los siguientes términos usados en este protocolo tendrán el significado que a continuación expresa:

1. **Anuncio Público**: A menos que no se especifique de otro modo, se considerará anuncio público para los fines de este Reglamento, cualquier comunicación escrita de la agencia, incluyendo, un comunicado de prensa o entrevista radial.

2. **Archivo de Información Personal**: se refiere a un expediente que contenga al menos el nombre o primera inicial y el apellido paterno de una persona, combinado con cualquiera de los siguientes datos de tal manera que se puedan asociar los unos con los otros y en el que la información sea legible sin necesidad de usar para acceder a ella una clave criptográfica especial:

   a) Número de Seguro Social;
   b) Número de Licencia de Conducir, Tarjeta Electoral u otra Identificación Oficial;
   c) Números de cuentas bancarias o financieras de cualquier tipo, con o sin las claves de acceso, que puedan habérsele asignado;
   d) Nombre de usuarios y claves de acceso a sistemas informáticos, públicos o privados;
   e) Información médica protegida por la Ley HIPAA;
   f) Información contributiva;

g) Evaluaciones laborales.

No se incluye dentro de la información protegida la dirección postal o residencial ni información que sea documento público y esté disponible para la ciudadanía en general.

3. **Bancos de Información:** Lugar donde se almacene, guarde o custodie cualquier tipo de documento, tanto electrónico como físico, por ejemplo: expedientes, tarjeteros, material audiovisual, entre otros.

4. **Ciudadano:** Incluye aquellas personas que aunque residen fuera de Puerto Rico mantienen información personal en las agencias en Puerto Rico.

5. **Clave Criptográfica:** escritura usando el arte de escribir con clave secreta o de un modo enigmático.

6. **Clientela:** Todo residente de Puerto Rico que tenga su información personal en bancos de información, cuyo propietario o custodio sea una entidad según definida en esta Regla.

7. **Entidad:** Corporación, institución, compañía o colectividad considerada como persona jurídica, y que sea propietaria o custodia de bancos de información que incluyan información personal de los residentes en Puerto Rico.

8. **Notificación:** A menos que no se especifique de otro modo en las reglas posteriores, se considerará notificación para los fines de este protocolo, cualquier comunicación escrita o verbal del Departamento, incluyendo sin limitar, un comunicado de prensa o entrevista radial.

9. **Persona:** Incluye las personas naturales y jurídicas.

10. **Procuradora:** Procuradora de la Oficina del Procurador del Ciudadano.

11. **PESSBIG:** Procuraduría Especializada de Sistemas de Seguridad de Bancos de Información del Gobierno.

12. **Robo de Identidad:** Cuando la información personal (identificable, financiera o médica) de un individuo ha sido obtenida y utilizada sin su consentimiento y con el propósito de cometer actividades fraudulentas.

13. **Violación de la Seguridad:** significa cualquier situación en que se detecte que se ha permitido el acceso de personas o entidades no autorizadas a los archivos de datos de modo que la seguridad, confidencialidad o integridad de la información en el banco de datos quede en entredicho; o cuando haya este acceso por personas o entidades normalmente autorizadas y se sepa o haya sospecha razonable que han violado la confidencialidad profesional u obtuvieron su autorización bajo falsas representaciones con la intención de hacer uso ilegal de la información. Incluye tanto el acceso a los bancos de información a través del sistema, como el acceso físico a los medios de grabación que los contienen y cualquier sustracción o movimiento indebido de dichas grabaciones.

III. OBLIGACIONES Y RESPONSABILIDADES

A. Toda entidad propietaria o custodia de un banco de información para uso comercial que incluya información personal de ciudadanos residentes en Puerto Rico deberá notificar a dichos ciudadanos de cualquier violación de la seguridad cuando los bancos de datos cuya seguridad fue violada contuvieran todo o parte de su archivo de información personal y la misma no estuviera protegida con claves criptográficas más allá de una contraseña.

B. Toda entidad que dentro de sus funciones revenda o provea acceso a bancos de información digitales que a su vez contengan archivos de información personal de ciudadanos deberá notificar al propietario, custodio o tenedor de dicha información de cualquier violación de la seguridad del sistema que haya permitido el acceso a aquellos archivos por personas no autorizadas.

Además, las entidades deberán:

1. Detectar y contener incidentes con inmediatez.
2. Notificar al Departamento de Asuntos del Consumidor en 10 días calendarios.
3. Informar a los ciudadanos afectados en un máximo de 72 horas desde la confirmación.
4. Documentar todas las acciones y conservar evidencia.
5. Cooperar con las autoridades competentes.

IV. PROCEDIMIENTO DE NOTIFICACIÓN

A. GENERAL: La entidad, al detectar la violación de seguridad, debe activar su Comité de Seguridad o Computer Security Response Team (CSIRT por sus siglas en inglés) interno para luego determinar la naturaleza y el alcance del incidente. Las entidades responsables luego informarán a DACO dentro de un plazo improrrogable de diez (10) días calendarios y PESSBIG dentro de 24 horas de detectarse la violación de la seguridad del sistema. **Además, se notificará al Puerto Rico Innovation and Technology Service (PRITS) siguiendo sus guías y normas.**

La notificación de violación de la seguridad del sistema que haga la entidad deberá indicar, hasta donde lo permitan, las necesidades de cualquier investigación o caso judicial que se encuentre en curso, la naturaleza de la situación, el número de clientes potencialmente afectados, si se han radicado querellas criminales, qué medidas se está tomando al respecto y un estimado del tiempo y costo requerido para rectificar la situación.

La notificación a la clientela que habrá de hacer la entidad deberá ser de la manera más expedita posible, tomando en consideración la necesidad de las agencias del orden público de asegurar posibles escenas de delito y pruebas, así como de la aplicación de medidas necesarias para restaurar la seguridad del sistema.

En el caso que se sepa específicamente en qué se violó la confidencialidad de la información de un cliente identificable, dicho cliente tendrá derecho a conocer qué información fue objeto de la violación de confidencialidad.

Las entidades deben conservar sus registros y evidencia de las violaciones de seguridad por un periodo mínimo de 5 años.

B. PROCEDIMIENTO DE NOTIFICACIÓN A DACO (Flujograma 1)

1. Notificar al DACO por escrito dentro de 10 días calendarios.

2. La notificación deberá incluir:

   a) Fecha de la violación,
   b) Número estimado de ciudadanos afectados,
   c) Naturaleza del incidente,
   d) Medidas correctivas implementadas,
   e) Estimado de tiempo y costo de remediación.

C. PROCEDIMIENTO DE NOTIFICACIÓN A LA OFICINA DEL PROCURADOR DEL CIUDADANO (Flujograma 2)

1. La entidad notificará a la PESSBIG dentro de 24 horas. La notificación deberá incluir:
   a) Fecha de la violación,
   b) Número estimado de ciudadanos afectados,
   c) Detalles de la información comprometida,
   d) Medidas correctivas y mitigación adoptadas,
   e) Contacto designado para seguimiento.

D. PROCEDIMIENTO DE NOTIFICACIÓN A LAS PERSONAS AFECTADAS (Flujograma 3)

1. Si los datos personales están comprometidos y no cifrados, la notificación se hará:
   a) Vía correo postal o electrónico autentificado.

2. Si el número de afectados excede 100,000 o el costo supera $100,000:
   a) Aviso web prominente.
   b) Publicación en medios de prensa.
   c) Envío de volantes informativos.

3. Contenido mínimo:
   a) Descripción general del incidente,
   b) Datos potencialmente comprometidos,
   c) Medidas tomadas,
   d) Acciones que puede tomar el ciudadano,
   e) Información de contacto.

V. DISPOSICIONES FINALES

A. PENALIDADES

El incumplimiento podrá conllevar multas de $500 a $5,000 por cada violación, sin perjuicio de otras sanciones civiles o penales aplicables, por cualquier incumplimiento de las disposiciones de este protocolo, o de las órdenes y resoluciones emitidas al amparo de éste.

B. CLÁUSULA DE SEPARABILIDAD

Si cualquier parte, artículo, párrafo, disposición o cláusula de este protocolo fuera declarada inconstitucional o inválida por una sentencia judicial, dicha determinación no afectará ni invalidará el resto de este protocolo, sino que su efecto quedará limitado a la parte, artículo, párrafo, disposición o cláusula que hubiera sido declarada inconstitucional o inválida.

C. VIGENCIA

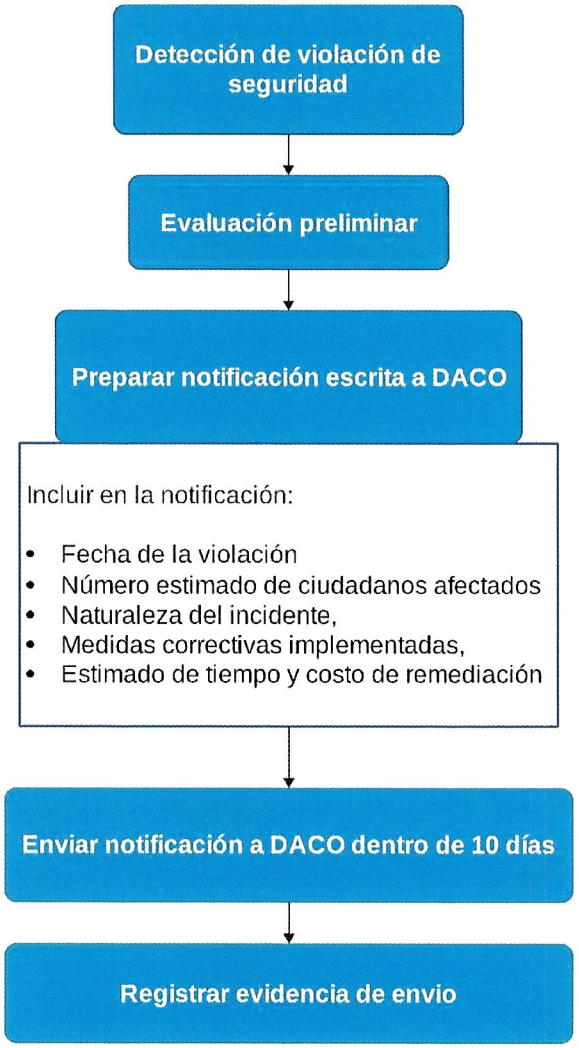
Este protocolo entrará en a la fecha de su aprobación.

Y PARA QUE ASÍ CONSTE, firmo y hago estampar en la misma el sello del Departamento de Agricultura del Gobierno de Puerto Rico, en la Ciudad de San Juan, Puerto Rico, hoy 13 de Agosto de 2025.

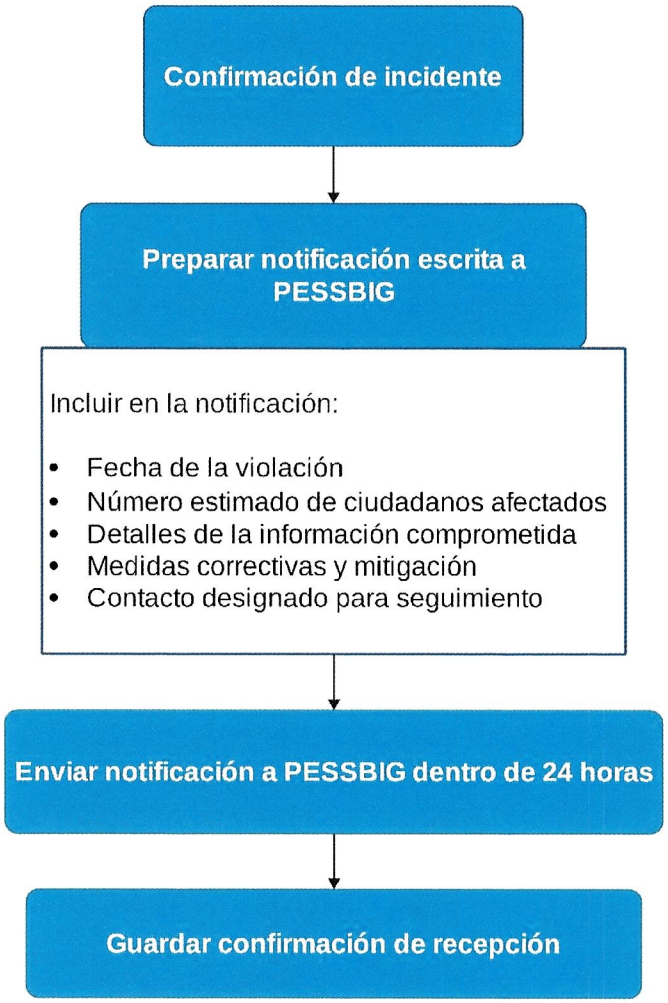
JOSUÉ E. RIVERA CASTRO
SECRETARIO

APÉNDICES

PROCEDIMIENTO DE NOTIFICACIÓN A DACO



PROCEDIMIENTO DE NOTIFICACIÓN A LA OFICINA DEL PROCURADOR DEL CIUDADANO



PROCEDIMIENTO DE NOTIFICACIÓN A LAS PERSONAS AFECTADAS