CDBG-DR

Política sobre Información de Identificación Personal, Confidencialidad y No Divulgación

(Política PII, por sus siglas en inglés)

Este documento es una traducción de la versión en inglés.
De haber alguna inconsistencia entre ambas versiones, la versión en inglés prevalecerá.

6 de marzo de 2020
V.1

Esta página se dejó en blanco intencionalmente.

DEPARTAMENTO DE LA VIVIENDA DE PUERTO RICO
PROGRAMA CDBG-DR
POLÍTICA SOBRE INFORMACIÓN DE IDENTIFICACIÓN PERSONAL, CONFIDENCIALIDAD Y NO DIVULGACIÓN
CONTROL DE VERSIONES

NÚMERO DE VERSIÓN	FECHA	DESCRIPCIÓN DE LA REVISIÓN
1	**6 de marzo de 2020**	**Versión original**

Índice

1 Introducción

El Departamento de la Vivienda de Puerto Rico (**Vivienda**), como administrador de fondos, está comprometido con un manejo responsable de los fondos de la Subvención en Bloque para Desarrollo Comunitario y Recuperación ante Desastres (**CDBG-DR**, por sus siglas en inglés). Como parte de su compromiso, Vivienda se esfuerza por proteger la privacidad de todas las partes interesadas. A través de los procesos de los programas CDBG-DR, el personal está, a menudo, expuesto o tiene acceso a información confidencial y/o sensitiva. Como resultado de lo anterior, se deben tomar las medidas adecuadas para garantizar que los documentos que incluyen información confidencial y/o sensitiva se manejen adecuadamente y estén protegidos contra el acceso no autorizado y el uso inadecuado de dicha información.

2 Alcance

La Política sobre Información de Identificación Personal, Confidencialidad y No Divulgación (Política PII) aplica a todos los empleados, personal, proveedores, distribuidores, suplidores, contratistas, subcontratistas, consultores, socios, solicitantes y recipientes del Programa CDBG-DR de Vivienda. Esta política garantiza que la información confidencial y/o sensitiva se mantenga protegida y sea utilizada de la manera adecuada y para el propósito previsto.

3 Propósito

El propósito de esta política es proteger el derecho a la confidencialidad y la protección de la información confidencial y/o sensitiva a través de todos los procesos de Vivienda y del Programa CDBG-DR. Al establecer la importancia de cumplir estrictamente con las medidas de confidencialidad, se infunde confianza y credibilidad en los programas CDBG-DR de Vivienda. Esta política también ayudará a proteger la información confidencial y/o sensitiva de los participantes, empleados, subrecipientes y contratistas del Programa CDBG-DR de Vivienda contra cualquier posible violación de la seguridad de la información.

4 Definiciones

Confidencialidad: La protección de información personal y/o sensitiva.

Contratista: Una compañía privada que produce bienes y servicios para las agencias gubernamentales mediante un contrato, subcontrato, orden de compra, acuerdo u otro arreglo similar.

FEMA: Se refiere a la Agencia Federal para el Manejo de Emergencias.

HUD: Se refiere al Departamento de la Vivienda y Desarrollo Urbano de los Estados Unidos.

Información confidencial y/o sensitiva: Se refiere a información sobre una persona o relativa a una empresa y que dicha persona o empresa no desea que se divulgue a personas o entidades no autorizadas.

Información de Identificación Personal (**PII,** por sus siglas en inglés)**:** Información que puede utilizarse para distinguir o rastrear la identidad de una persona, ya sea por sí misma o al combinarla con otra información personal o información de identificación que está vinculada o que se puede vincular a una persona en específico. 2 C.F.R. § 200.79. Información que se puede utilizar para distinguir o rastrear la identidad de una persona, lo que incluye su nombre, Seguro Social, registros biométricos, etc., ya sea por sí sola o combinada con otra información personal o información de identificación que está vinculada o que se puede vincular a una persona en específico, tal como su fecha y lugar de nacimiento, el apellido de soltera de la madre, etc.[1]

Información de identificación personal protegida: Significa el nombre, la inicial del segundo nombre y el apellido de una persona, en combinación con uno o más tipos de información, incluyendo, sin limitarse a, el número de Seguro Social, número del pasaporte, números de tarjetas de crédito, autorizaciones, números de cuentas bancarias, información biométrica, fecha y lugar de nacimiento, apellido de soltera de la madre, antecedentes penales, historial médico o financiero y transcripciones o expedientes académicos. La información de identificación personal protegida no incluye información cuya divulgación es requerida por ley. 2 C.F.R. § 200.82.

Información de identificación personal pública: Se define como información de identificación personal que está disponible en fuentes públicas, tales como guías telefónicas, sitios web públicos y listados de universidades. 2 C.F.R. § 200.79.

Información de identificación personal sensitiva: Es información de identificación personal que si se pierde, se ve comprometida o se divulga sin autorización puede perjudicar sustancialmente a una persona.[2] La información de identificación personal sensitiva puede abarcar información que, por sí sola, o en combinación con otro tipo de información puede identificar a una persona.

Información que no es de identificación personal (**Non PII**, por sus siglas en inglés)**:** Información que no es suficiente para distinguir o rastrear la identidad de la persona a quien pertenece la información.

No divulgación: El acto de no dar a conocer algo.

Solicitante: Una persona que ha solicitado asistencia de uno de los programas CDBG-DR.

Subrecipiente: Una agencia, autoridad u organización sin fines de lucro, pública o privada, o una organización de desarrollo comunitario que recibe fondos CDBG-DR del recipiente o de otro subrecipiente, para llevar a cabo actividades elegibles bajo el Programa CDBG-DR. 24 C.F.R. § 570.500(c). También se define en 2 C.F.R. § 200.93 como una entidad no federal que recibe una subadjudicación de una entidad conducto o entidad intermediaria("pass-through entity"), para llevar a cabo parte de un programa federal.

Violación a la seguridad de la informacón: Ocurre cuando una persona, que no es el propietario o que no está autorizada a acceder a la información de identificación personal como parte de sus deberes oficiales, ve, revela o tiene acceso a dicha información.

Vivienda: Se refiere al Departamento de la Vivienda de Puerto Rico.

---

[1] Memorando 07-16 de la OMB, sobre Cómo protegerse contra y responder a una violación de información de identificación personal, https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/memoranda/2007/m07-16.pdf

[2] Protecting PII Capacity Building Guidance on Protecting Privacy Information, U.S. Department of Housing and Urban Development [Guía para el desarrollo de la capacidad para proteger la información de identificación personal y la información privada, Departamento de la Vivienda y Desarrollo Urbano de Estados Unidos], abril de 2015, https://www.hud.gov/sites/documents/OHC_PII042815.PDF

5 Información de Identificación Personal (PII)

Es necesario establecer medidas especiales para ayudar a los esfuerzos que se llevan a cabo en las áreas afectadas por los desastres, con el fin de agilizar la prestación de ayuda, asistencia y servicios de emergencia, así como la reconstrucción y rehabilitación de las áreas devastadas. Al proveer programas de asistencia federal para cubrir pérdidas tanto públicas como privadas, el gobierno local puede desempeñar sus responsabilidades para aliviar el sufrimiento y los daños causados por el desastre. 42 U.S.C. § 5121(b)(6).

Para implementar estos programas de asistencia federal, Vivienda, como administrador de los fondos CBDG-DR, necesita recopilar, mantener, utilizar, recuperar y difundir información relacionada con las personas que solicitan asistencia financiada con fondos CDBG-DR. Debido a la naturaleza de los programas, los expedientes de los Solicitantes pueden contener información sobre sus ingresos, seguros, informes de inspección de viviendas y anotaciones sobre distintos tipos de asistencia. Parte de la información incluida en los registros de los Solicitantes, sino toda, se considera como información de identificación personal.

La información de identificación personal se refiere a información que se puede utilizar para distinguir o rastrear la identidad de una persona, ya sea por sí sola o en combinación con otro tipo de información personal o información de identificación que está vinculada o que puede vincularse a una persona en específico. Dada la naturaleza de la información personal, la definición de información de identificación personal es necesariamente amplia y no se basa en una sola categoría de información o tecnología. En cambio, requiere de un análisis caso a caso sobre el riesgo específico de que se puede identificar a una persona usando cierto tipo de información.[3] Por ejemplo, la información que no es de identificación personal se puede convertir en información de identificación personal cuando, al combinarla con otra información que ha estado disponible públicamente (sin importar el medio o la fuente), esta podría usarse para identificar a una persona. 2 C.F.R. § 200.79. La información de identificación personal es un tipo de información sensitiva, que incluye, sin limitarse a, la información de identificación personal y la información de identificación personal sensitiva.[4]

[3] Memorando 17-12 de la OMB, sobre Cómo prepararse y responder a una violación de información de identificación personal, 2 de enero de 2017, https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/memoranda/2017/m-17-12_0.pdf

[4] Información sensitiva es cualquier información que si se pierde, se utiliza de forma indebida o se divulga, o si se accede o se modifica sin autorización, puede perjudicar sustancialmente la seguridad o los intereses nacionales o internos, la ejecución de programas federales o la privacidad de las personas, pero para la cual no se ha autorizado específicamente, bajo los criterios de una Orden Ejecutiva o una Ley del Congreso, que se mantenga en secreto por el bien de la defensa nacional, la seguridad interna o la política extranjera. Directriz 4300A del Departamento de Seguridad Nacional sobre Sistemas Sensitivos, versión 13.1, 27 de julio de 2017.

Los empleados y el personal del Vivienda y del programa CDBG-DR que manejan información de identificación personal deben ejercer un cuidado especial. Debido a la naturaleza abarcadora de la definición de información de identificación personal, el contexto es muy importante al momento de determinar el alcance de las medidas de protección empleadas. No obstante, al manejar información de identificación personal, es más seguro ser precavidos.

5.1 Tipos de Información de Identificación Personal

5.1.1 Información de Identificación Personal Pública

La información de identificación personal pública se define como información que está disponible en fuentes públicas, tales como directorios de teléfonos, sitios web públicos y listados de universidades. 2 C.F.R. § 200.79. Los ejemplos de información de identificación personal pública incluyen:

- Nombre y apellido;
- Dirección;
- Número de teléfono del trabajo;
- Dirección de correo electrónico;
- Número de teléfono residencial; y
- Credenciales académicos en general.

Como regla general, la información de identificación personal pública no está sujeta a las medidas de protección rigurosas que se aplican a la información de identificación personal protegida y sensitiva, ya que no se le considera lo suficientemente sensitiva para requerir protección. No obstante, la determinación de que cierta información de identificación personal no es sensitiva no significa que se puede divulgar al público.

5.1.2 Información de Identificación Personal Sensitiva y Protegida

La información sensitiva es información de identificación personal que, si se pierde, se ve comprometida o se divulga sin autorización, podría *perjudicar sustancialmente* a una persona.[5] La información de identificación personal sensitiva puede abarcar información capaz de identificar a una persona, por sí sola, o en combinación con otro modo de identificación.

Los siguientes son ejemplos de información de identificación personal sensitiva que pueden identificar a una persona por sí solos:

- Números de Seguro Social o números de identificación comparables;
- Información financiera relacionada con las personas; e
- Información médica relacionada con las personas.

[5] Protecting PII Capacity Building Guidance on Protecting Privacy Information, U.S. Department of Housing and Urban Development [Guía para el desarrollo de la capacidad para proteger la información de identificación personal y la información privada, Departamento de la Vivienda y Desarrollo Urbano de Estados Unidos], abril de 2015, https://www.hud.gov/sites/documents/OHC_PII042815.PDF

Los siguientes son ejemplos de información que, al combinarla con otro tipo de información de identificación, se convierte en información de identificación personal sensitiva:

- Ciudadanía o estatus migratorio;
- Información médica;
- Afiliación étnica o religiosa;
- Orientación sexual;
- Contraseñas de cuentas;
- Últimos cuatro (4) dígitos del número de Seguro Social;
- Fecha de nacimiento;
- Antecedentes penales; y
- Apellido de soltera de la madre.

Al ser una subdivisión de la información de identificación personal, la información de identificación personal sensitiva requiere niveles adicionales de controles de seguridad. Además, conlleva procedimientos de manejo más estrictos, ya que supone un riesgo mayor para una persona si dicha información se accede de forma inadecuada o se ve comprometida. En la medida posible, como parte de los requisitos programáticos establecidos por el Departamento de Vivienda y Desarrollo Urbano de Estados Unidos (**HUD**, por sus siglas en inglés) y en cumplimiento con la Ley de Privacidad de 1974, 5 U.S.C. § 552(a), la recopilación, mantenimiento, uso y divulgación de números de Seguro Social, números de identificación patronal, cualquier información derivada de estos e información sobre ingreso se llevará a cabo, según aplique, de conformidad con la Ley de Privacidad y todas las disposiciones aplicables de las leyes federales, estatales y locales. 24 C.F.R. § 5.212.

Según se define en esta Política, la información de identificación personal protegida se refiere al nombre o inicial y el apellido de una persona, cuando se combina con uno o más tipos de información, que incluye, pero no se limita a, el número de Seguro Social, número de pasaporte, números de tarjetas de crédito, autorizaciones, números de cuentas bancarias, información biométrica, fecha y lugar de nacimiento, apellido de soltera de la madre, antecedentes penales, expedientes médicos y financieros o transcripciones o expedientes académicos. La información de identificación personal protegida no incluye información cuya divulgación es requerida por ley. 2 C.F.R. § 200.82. Según lo indica su definición, la información de identificación personal protegida está englobada en la definición de información de identificación personal sensitiva cuando la información que normalmente no es sensitiva se combina con otra información y, por ende, se convierte en información de identificación personal sensitiva y protegida.

5.2 Acceso y Manejo de la Información de Identificación Personal

En la implementación, manejo y ejecución de los Programas CDBG-DR, el personal de Vivienda y sus subrecipientes, contratistas y agencias asociadas recopilarán, utilizarán,

almacenarán, difundirán, encontrarán y tendrán acceso a una cantidad sin precedentes de información personal de los solicitantes.

Como medida de control interno al manejar fondos de adjudicaciones federales, todas las entidades no federales deben "[t]omar medidas razonables para proteger la información de identificación personal protegida y demás información que la agencia federal adjudicadora o entidad intermediaria designó como sensitiva o que la entidad no federal considera sensitiva de acuerdo con las leyes federales, estatales, locales y tribales aplicables, relacionadas con la privacidad y las obligaciones de confidencialidad". 2 C.F.R. § 200.303(e).

De acuerdo con lo estipulado en 2 C.F.R. § 200.303, con respecto a los controles internos de las entidades no federales, Vivienda ha establecido sistemas para la protección de la información de identificación personal obtenida. Estos sistemas incluyen el manejo de nombres de usuario y contraseñas, archivos y expedientes físicos y digitales, uso de programas, aplicaciones y software, etc. Esta Política incluye las mejores prácticas sugeridas para estos casos.

5.2.1 Confidencialidad y No divulgación

Se espera que Vivienda proteja la información que le han confiado las personas que buscan asistencia del Programa CDBG-DR. El derecho a la privacidad y a la protección de información personal está establecido en el Código Penal de Puerto Rico de 2012, 33 LPRA § 5021 *et seq.* El Artículo 173 del Código Penal establece que toda persona que difunda, publique, revele o ceda a un tercero los datos, comunicaciones o hechos descubiertos o las imágenes captadas a que se refieren los artículos 171[6] y 172[7] de este Código, u ofreciere o solicitare tal distribución o acceso, será sancionada. 33 LPRA § 5239.

La Ley de Datos Abiertos del Gobierno de Puerto Rico, Ley 122-2019, dispone como política pública del Gobierno de Puerto Rico que el manejo efectivo de los datos del gobierno es esencial para dar apoyo a los procesos de innovación de todos los sectores, para facilitar una cultura de mejoramiento continuo y rendición de cuentas, para un desarrollo y crecimiento económico sostenible, y para generar resultados tangibles, valiosos y de impacto para los ciudadanos. Las excepciones del deber de

[6] El Artículo 171 se refiere a violaciones contra las comunicaciones personales; toda persona que sin autorización y con el propósito de enterarse o permitir que cualquiera otra se entere, se apodere de los papeles, cartas, mensajes de correo electrónico o cualesquiera otros documentos o efectos de otra persona, o intercepte sus telecomunicaciones a través de cualquier medio, o sustraiga o permita sustraer los registros o récords de comunicaciones, remesas o correspondencias cursadas a través de entidades que provean esos servicios, o utilice aparatos o mecanismos técnicos de escucha, transmisión, grabación o reproducción del texto, sonido, imagen, o de cualquier otra señal de comunicación, o altere su contenido será sancionada. A los fines de esta sección, el hecho de que la persona tuviere acceso a los documentos, efectos o comunicaciones a que se hace referencia dentro de sus funciones oficiales de trabajo no constituirá de por sí "autorización" a enterarse o hacer uso de la información más allá de sus estrictas funciones de trabajo. 33 LPRA § 5237.

[7] El artículo 172 se refiere a la alteración y uso de datos personales en archivos. Toda persona que, sin estar autorizada, se apodere, utilice, modifique o altere, en perjuicio del titular de los datos o de un tercero, datos reservados de carácter personal o familiar de otro que se hallen registrados en discos o archivos informáticos o electrónicos, o en cualquier otro tipo de archivo o registro público o privado, será sancionada con pena de reclusión por un término fijo de tres (3) años. Si la persona convicta es una persona jurídica será sancionada. 33 LPRA § 5238.

confidencialidad que impone esta Ley incluyen que la información esté protegida por ley, que revelar los datos podría causar daños a terceros, que la divulgación de dicha información podría invadir la privacidad de un tercero y que toda la información relacionada con la dirección física, número de teléfono, información de contacto de emergencia, número de Seguro Social, número de tarjeta de crédito, información financiera o de impuestos, actividad bancaria e información confidencial de terceros privados. Ley 122-2019, Art. 4.

Las partes involucradas en el Programa CDBG-DR de Vivienda acordarán tomar pasos o medidas razonables para proteger la información confidencial o sensitiva y no utilizarán, mercadearán ni divulgarán información confidencial o sensible sin la autorización expresa por escrito de la parte afectada. Los contratistas y subcontratistas del Programa CDBG-DR de Vivienda deben cumplir con la cláusula de confidencialidad y no divulgación dispuesta en sus contratos.

5.2.2 Terminación del empleo y Acceso a la Información

El proceso de separación de un empleado de una empresa ("offboarding") involucra a las divisiones de Recursos Humanos, Operaciones, Tecnología Informática (**IT**, por sus siglas en inglés) y cualquier otra área identificada en la cual el empleado o miembro del personal tiene o ha tenido acceso a expedientes, discos de almacenamiento de datos, aplicaciones o cualquier otro método de manejo de información. Durante este proceso, estas áreas trabajarán en conjunto para identificar la información, discos o aplicaciones a los que el empleado tiene o ha tenido acceso, con el fin de desactivar todas las credenciales y privilegios de acceso que le fueron asignados. El supervisor del empleado o el director de la división son los responsables de notificar al Departamento de IT y solicitar la eliminación de los privilegios de acceso mediante un "Formulario de Solicitud de Acceso a la Red", el cual enviarán al Departamento de IT.[8] Si un dispositivo electrónico o teléfono celular de un empleado contiene aplicaciones que sincronizan la información de correos electrónicos, contactos, calendarios y discos de almacenamiento remoto de datos, estos deberán verificarse y desactivarse de inmediato. Mediante el proceso de separación de un empleado, Vivienda llevará a cabo lo siguiente:

- Reforzar la importancia de la confidencialidad;
- Solicitar toda la información que todavía esté en posesión del empleado;
- Solicitar todos los aparatos electrónicos que pertenezcan a Vivienda, tales como tabletas y computadoras portátiles; y
- Recoger las llaves, tarjetas de identificación y demás dispositivos de acceso que posea el empleado.

5.2.3 Consentimiento por escrito y Persona designada para las comunicaciones

[8] Políticas de Seguridad Informática del Programa CDBG-DR de Vivienda, 23 de agosto de 2019, página 13.

La información del Solicitante está sujeta a la Ley de Privacidad de 1974: "[l]a información personal solo puede ser utilizada por personas autorizadas en el desempeño de funciones oficiales". El uso de información se limitará a garantizar el cumplimiento de los requisitos del programa, las regulaciones federales y regulaciones de HUD; reducir los errores y mitigar el fraude y el abuso; y esta información solo se divulgará a las personas a quienes el Solicitante ha autorizado por escrito. Se debe obtener consentimiento de las partes involucradas al divulgar información confidencial o sensitiva respecto un participante, empleado o contratista del programa CDBG-DR de Vivienda. El Formulario de Consentimiento revela los detalles que compartirá la parte afectada y llevará su firma y la fecha. Algunos programas CDBG-DR permiten a los Solicitantes designar a un tercero para obtener información sobre su solicitud al Programa. Este tercero se conoce como la persona designada para las comunicaciones. La persona designada para las comunicaciones sirve como punto de contacto para el Solicitante y no actúa bajo un Poder notarial. Esta persona designada puede obtener y proveer información al Programa a nombre del Solicitante. No obstante, no pueden firmar ningún documento ni establecer ningún acuerdo, a menos que no les hayan otorgado la autoridad mediante un Poder notarial.

Los empleados, contratistas y demás personal solo deben tener acceso a información confidencial o sensitiva de sus propios programas. Las guías del programa incluyen disposiciones que garantizan la confidencialidad de los solicitantes de los programas, así como la protección y la preservación de los expedientes. Una excepción a la limitación de acceso a información confidencial o sensitiva, contempla la necesidad de proveer acceso a las agencias u organismos de monitoreo y supervisión federales o locales, así como a su personal. Las actividades de monitoreo y supervisión son muy importantes para ayudar a Vivienda en la implementación adecuada de los programas y fondos CDBG-DR. A pesar de esta excepción, todo empleado al que se le concede acceso a archivos, documentos, computadoras y otros dispositivos que contengan información de identificación personal deben ejercer el mismo grado de cautela que cualquier otro empleado, subrecipiente o contratista del Programa CDBG-DR de Vivienda. La información divulgada debe limitarse al programa o área específica que se encuentra bajo supervisión o monitoreo, y todas las actividades de acceso electrónico deben contar con funciones y privilegios diseñados a la medida que permitan monitorear y llevar un registro de la información a la que se tiene acceso.

En cumplimiento con lo dispuesto en 2 C.F.R. § 200.303, el personal que tiene acceso a información confidencial o sensitiva es responsable de tomar las medidas necesarias para proteger adecuadamente los equipos, expedientes, contraseñas y comunicaciones manejadas. Los empleados, contratistas, agencias asociadas, personal y otras personas con acceso a información confidencial o sensitiva de Vivienda y de los Subrecipientes deben completar un Acuerdo de Confidencialidad y/o un Acuerdo de No Divulgación. Este acuerdo forma parte del expediente del empleado, contratista, agencia asociada o personal, así como un acuse de recibo de esta Política.

En resumen, este acuerdo establece que ninguna de las partes, ni ninguno de sus empleados, divulgará o revelará datos o información desarrollada u obtenida a raíz de su relación contractual. El personal deberá garantizar el manejo adecuado de todos los documentos y expedientes impresos y deberá establecer parámetros para el manejo de información confidencial o sensitiva.

Como parte del Programa CDBG-DR, Vivienda y los subrecipientes emplearán y mantendrán distintos métodos para informar a los solicitantes sobre el estatus de sus solicitudes de asistencia para recuperación durante las distintas fases del programa. Se utilizarán múltiples métodos de comunicación estándar, tales como correo postal y correo electrónico, entre otros, para garantizar que los solicitantes reciban información precisa y a tiempo con respecto a sus solicitudes. Por lo tanto, según se establece en esta Política, Vivienda ha establecido medidas para proteger la información de identificación personal y capacitará y brindará asistencia a los empleados y subrecipientes en cuanto a la implementación de estrategias equivalentes para la protección de la información de identificación personal.

5.2.4 Recopilación e intercambio de Información de Identificación Personal

El derecho a la privacidad y el control sobre la información personal de un Solicitante están esbozados en la Constitución del Estado Libre Asociado de Puerto Rico. Artículo II, Sección 8, de la Constitución de Puerto Rico (1952). Como parte de dicha protección constitucional, es de interés para el Estado salvaguardar el derecho de las personas a su dignidad, intimidad e integridad personal.

En general, HUD establece su compromiso de proteger la privacidad de la información de las personas, ya sea almacenada electrónicamente o impresa, de acuerdo con las leyes, directrices y mejores prácticas federales. HUD espera que sus socios comerciales que recopilan, utilizan, mantienen o difunden información de HUD, entre estos, las Autoridades de Vivienda Pública, protejan la privacidad de dicha información de acuerdo con las leyes aplicables. [9]

Para garantizar el cumplimiento con la información de identificación personal y las políticas y procedimientos de confidencialidad, la recopilación de información de identificación personal sensitiva debe limitarse a tales propósitos. Dicha información no debe recopilarse ni mantenerse sin la debida autorización. En la medida de lo posible, la información personal que se utiliza para determinar los derechos, beneficios y/o privilegios de un Solicitante, debe obtenerse directamente de la persona.

Las leyes de Puerto Rico disponen para la protección y recopilación del número de Seguro Social por parte de las agencias, dependencias e instrumentalidades del Gobierno de Puerto Rico y sus tres ramas, sus municipios, corporaciones públicas y sus

[9] Declaración de privacidad incluida en los distintos programas financiados por el HUD – La declaración se extrajo de un contrato para un proyecto de Sección 8, https://www.hud.gov/sites/dfiles/OCHCO/documents/52530Bpt1.pdf

contratistas (entre otros), dentro de parámetros determinados y para los medios estipulados y autorizados por las leyes federales.

La Ley para Disponer sobre el Uso del Número de Seguro Social en los Procesos de Provisión de Servicios, o de Subastas y Contrataciones con el Gobierno de Puerto Rico, o de Donativos y Transferencias de Fondos Públicos, Ley 187-2006, según enmendada, 18 LPRA § 926(f), establece como requisito para contratar con el gobierno, que las entidades privadas deben garantizar a todos los ciudadanos que no difundirán, desplegarán o revelarán su número de Seguro Social en documentos que estén accesibles o visibles a personas no autorizadas.

La Ley para Prohibir el Uso del Número de Seguro Social de un Empleado en las Tarjetas de Identificación o en Cualquier Documento de Circulación General o Rutinaria, Ley 27-2006, 29 LPRA § 621a, dispone que ningún patrono, de empresa privada o de corporación pública del Estado Libre Asociado de Puerto Rico, podrá mostrar o desplegar el número de Seguro Social de un empleado en su tarjeta de identificación, ni podrá mostrar o desplegar este dato en ningún lugar visible al público en general o documento de circulación general. Las protecciones otorgadas por la citada ley pueden ser renunciadas por el empleado, siempre y cuando la renuncia sea voluntaria y por escrito. Ahora bien, la renuncia no podrá imponerse como condición de empleo. Como excepciones a la aplicación de las disposiciones de la Ley 27-2006, se encuentran aquellos casos o fines para los cuales es compulsorio, por ley, el uso del número de Seguro Social, o se ha autorizado o regulado mediante ley o reglamento federal. Tampoco aplicarán las disposiciones de esta ley cuando el uso del número de Seguro Social sea para propósitos de verificación de identidad, contribuciones, contratación y nóminas, sujeto a que el patrono tome las medidas de seguridad adecuadas para mantener su confidencialidad.

Ley para Disponer la Política Pública sobre el Uso del Número de Seguro Social como Verificación de Identificación y la Protección de su Confidencialidad, y Disponer los Límites y Requisitos para el Uso de Este Dato, Ley 243-2006, según enmendada, 29 LPRA § 621(b), dispone, en su Artículo 3, que las entidades referidas "podrán recopilar el Número de Seguro Social de las personas con quienes hagan transacciones oficiales y hacer uso del mismo para fines de facilitar el cotejo de verificación de identidad, hacer contrarreferencia con la información disponible internamente o en otras agencias o entidades […], y para uniformar los procedimientos internos de intercambio de información". También establece limitaciones y prohibiciones, así como las medidas generales que el Estado deberá adoptar para salvaguardar la confidencialidad de la información.

5.2.5 Acuerdos de Intercambio de Información

Como parte de los esfuerzos para recuperación ante desastres, Vivienda trabaja con las agencias federales y locales, socios y subrecipientes para ampliar su alcance. Estas colaboraciones requieren que estas agencias, socios y subrecipientes compartan

información, lo que, en muchas ocasiones, incluye información de identificación personal sensitiva y protegida. Con el fin de imponer directrices claras, Vivienda ha establecido acuerdos para el intercambio de información. Estos acuerdos definen las responsabilidades de las partes para proteger, manejar y compartir la información de identificación personal.

Una de las medidas de Vivienda para la recuperación ante desastres ha sido su participación en un Acuerdo de Intercambio y Acceso de Información (**ISAA**, por sus siglas en inglés) con la Agencia Federal para el Manejo de Emergencias (**FEMA**). Mediante una enmienda al ISAA[10] original, FEMA permitió a Vivienda compartir información de identificación personal con sus contratistas. Este acuerdo, así como otros acuerdos de intercambio de información, pueden sufrir enmiendas cada cierto tiempo, así como de prórrogas, para ampliar su período de vigencia. Según se establece en DHS/FEMA 008 – Disaster Recovery Assistance Files System of Records [Sistema de Registros de Archivos de Asistencia para Recuperación ante Desastres][11], este sistema permite al Departamento de Seguridad Nacional (**DHS**, por sus siglas en inglés) y a FEMA recopilar y mantener registros de los solicitantes a programas de asistencia ante desastres que ofrecen asistencia financiera u otro tipo de ayuda tangible a los sobrevivientes de desastres declarados por el Presidente de los Estados Unidos.

Por lo general, los Acuerdos de Intercambio de Información incluyen, como mínimo, las siguientes cláusulas:

- La información de identificación personal debe compartirse y transmitirse de una forma segura que reduzca la probabilidad de una violación de la seguridad de la información.
    - Si se va a utilizar una plataforma, aplicación u otra herramienta especial, deberán incluirse cláusulas sobre las credenciales de acceso (nombre de usuario y contraseñas), instrucciones para usuarios, manuales y manejo y protección adecuada de la información de identificación personal.
    - Las credenciales de acceso no se deben compartir con personal no autorizado o empleados del Programa CDBG-DR.
- Las partes deberán garantizar la exactitud de la información.
- La información de identificación personal solo debe utilizarse para dirigir los objetivos del Programa.
- Se instruirá a las personas que manejarán o tendrán acceso a la información de identificación personal en cuanto a la naturaleza confidencial de la información

[10] El Acuerdo original de Intercambio y Acceso a la Información entre la Agencia Federal para el Manejo de Emergencias del Departamento de Seguridad Nacional y el Departamento de la Vivienda de Puerto Rico para el huracán Irma, FEMA -4336-DR, y el huracán María, FEMA-4339-DR, se firmó en noviembre de 2017. La segunda enmienda a este acuerdo se firmó en mayo de 2019.

[11] DHS/FEMA 008 – Disaster Recovery Assistance Files System of Records [Sistema de Registros de Archivos de Asistencia para Recuperación ante Desastres], DRA_78 Ded. Reg. 25, 28 (Apr. 30, 2013) (DRA SORN). El documento está disponible en: https://www.govinfo.gov/content/pkg/FR-2013-04-30/html/2013-10173.htm.

y las repercusiones penales o civiles que podrían enfrentar por el mal manejo de información sensitiva o protegida.

- Deberán emplear medidas de seguridad técnicas, físicas y administrativas adecuadas para proteger la información de identificación personal.
- Cumplimiento con los requisitos y regulaciones incluidas en la Parte 200 del Título 2 del Código de Regulaciones Federales (2 C.F.R. Part 200).
- Asegurarse de que los sistemas basados en internet ("cloud-based") cumplan o excedan los requisitos básicos de controles de privacidad y seguridad aplicables a los sistemas del Gobierno Federal.
    - Estos sistemas deben ser objeto de un monitoreo constante para asegurar que operen en la última versión actualizada.
- Limitar el acceso a la información de identificación personal a los empleados que administran la asistencia.
- Prohibir la divulgación de información de identificación personal a terceros sin consentimiento por escrito.
- Asegurarse de que el personal con acceso a la información de identificación personal complete los talleres de capacitación sobre privacidad y seguridad y entienda lo que conlleva la protección de la información de identificación personal.
- En caso de una sospecha o de un incidente real relacionado con la seguridad, se deberá emitir, de inmediato, un Aviso de Incidente de Seguridad.
- El cumplimiento de las cláusulas se extenderá a todos los contratistas que tengan acceso a la información de identificación personal.

5.2.6 Métodos para la transmisión segura de Información de Identificación Personal

En ocasiones, será necesario transmitir información de identificación personal a otra persona, agencia, personal del programa, etc. La información de identificación personal solo debe transmitirse tomando como base el principio de la necesidad de tener conocimiento. No obstante, se deben tomar varias precauciones al momento de compartir esta información para evitar incidentes de filtración de la información de identificación personal.

Al compartir información de identificación personal, es necesario tomar ciertas medidas de seguridad para proteger la información sensitiva. Por ejemplo, si la información se envía por correo electrónico o a través de un sistema no seguro, el uso de medidas de protección adecuadas, tales como el cifrado o codificación de los documentos adjuntos al mensaje, es necesaria. Como medida de precaución, se debe utilizar un programa cifrado "encryption software", en las computadoras diseñadas para la transmisión de información de identificación personal, la información de identificación personal sensitiva debe cifrarse antes de enviarse, la transmisión debe hacerse utilizando aplicaciones de internet seguras y asegurarse de que se hayan establecido los protocolos correspondientes. Si la información se va a enviar por fax, debe confirmarse

el número de fax, el destinatario deberá estar esperando el documento y ninguna persona no autorizada deberá interceptar el envío. La información de identificación personal no se colocará en discos de almacenamiento compartidos, intranet o internet y los documentos impresos no deberán dejarse sobre un escritorio, una impresora o en áreas donde el personal no autorizado pueda tener acceso a la información. Otras medidas de protección incluyen lo siguiente:

- La información de identificación personal solo se debe compartir tomando como base el principio de la necesidad de tener conocimiento.[12]
- La información de identificación personal solo debe distribuirse cuando se autorice mediante un consentimiento por escrito.
- La información de identificación personal solo debe discutirse por teléfono luego de confirmar que la persona está autorizada para discutir dicha información.
- No se debe incluir información de identificación personal en mensajes de voz, en ningún medio de comunicación.
- La información de identificación personal no debe discutirse en público ni en espacios compartidos donde personas no autorizadas pueden escuchar la conversación.
- Las reuniones en las que se discutirá información de identificación personal deben celebrarse en espacios seguros.
- Las minutas de estas reuniones deben considerarse como confidenciales si contienen información de identificación personal.[13]

5.2.7 Eliminación de la Información de Identificación Personal

Los expedientes que contienen información de identificación personal no deben conservarse por más tiempo del requerido por las normas de los programas y los estatutos locales. Una vez que se cumplen estos plazos de tiempo, se deben destruir los expedientes. La disposición adecuada de información de identificación personal sensitiva conlleva la eliminación permanente de los expedientes electrónicos y la trituración de los expedientes impresos.[14] Vivienda exige que el personal, los contratistas y los subrecipientes del Programa CDBG-DR eliminen adecuadamente la información de identificación personal sensitiva, de acuerdo con los plazos establecidos para la conservación de archivos, de manera que no se pueda leer ni reconstruir la información. Los métodos de eliminación aceptables incluyen la trituración, quema o pulverización de papel y la destrucción de los medios o la remoción permanente de los datos de

[12] Directriz Administrativa del del Departamento de Seguridad Nacional 11042.1: La protección de información sensible pero no confidencial (para uso oficial solamente) define la *necesidad de conocimiento* como la determinación tomada por el poseedor de la información de que un posible recipiente necesita acceso a información específica para poder desempeñar o brindar asistencia a una función gubernamental legal y autorizada, es decir, que necesita acceso para el desempeño de sus deberes oficiales. El documento está disponible en: https://www.dhs.gov/sites/default/files/publications/Management%20Directive%2011042.1%20Safeguarding%20Sensitive%20But%20Unclassified%20%28For%20Official%20Use%20Only%29%20Information_0.pdf

[13] Protecting PII Capacity Building Guidance on Protecting Privacy Information, U.S. Department of Housing and Urban Development [Guía para el desarrollo de la capacidad para proteger la información de identificación personal y la información privada, Departamento de la Vivienda y Desarrollo Urbano de Estados Unidos], abril de 2015, https://www.hud.gov/sites/documents/OHC_PII042815.PDF.

[14] Id.

información de identificación personal de los dispositivos de almacenaje. El desecho de computadoras y dispositivos portátiles de almacenaje debe incluir el uso de software para borrar datos de los discos duros de forma segura, de manera que los datos no puedan recuperarse.

5.2.8 Contratistas y subrecipientes

Vivienda espera que los socios, subrecipientes, consultores y contratistas del Programa CDBG-DR, así como sus empleados, se rijan por esta Política. Cuando un contratista o subrecipiente utiliza u opera sistemas de información de identificación personal o crea, recopila, utiliza, almacena, mantiene, difunde, divulga o dispone de información de identificación personal dentro del alcance de los fondos CDBG-DR, Vivienda deberá asegurarse de que los contratistas o subrecipientes adopten y administren esta Política adecuadamente. Los contratos y los acuerdos con subrecipientes del Programa CDBG-DR de Vivienda contienen cláusulas o disposiciones que protegen contra la divulgación y uso inadecuado de información confidencial o sensitiva. Los contratistas no utilizarán, venderán, mercadearán ni divulgarán información confidencial o sensitiva a un tercero, sin el consentimiento por escrito del Secretario de Vivienda. A través de las políticas y acuerdos de confidencialidad y no divulgación, Vivienda y los Programas CDBG-DR establecen prácticas justas sobre el uso de la información para garantizar que la información personal sea correcta, relevante y vigente; que los usos de la información sean conocidos y adecuados y que se proteja la información personal o sensitiva.

Las medidas de acción que constituyen las mejores prácticas incluyen:

- Verificación de referencias o de antecedentes de los empleados del Programa CDBG-DR que tendrán acceso a información de identificación personal sensitiva;
- Acuse de recibo de políticas y procedimientos sobre información de identificación personal por parte de los empleados (mediante los Avisos de Alerta de Política, talleres de capacitación, etc.);
- Restringir el acceso a la información de identificación personal;
- Capacitación sobre la información de identificación personal;
- Tapar o eliminar la información de identificación personal sensitiva en los acuerdos y contratos con subrecipientes;
- No divulgar la información provista por los solicitantes; y
- Responder y manejar adecuadamente a los incidentes de filtración de información.

Se espera que los contratistas manejen los datos y demás información que incluye información de identificación personal siguiendo estándares que cumplan o superen las normas establecidas en esta Política. Como parte del monitoreo de su Programa CDBG-DR, Vivienda verificará que los subrecipientes y contratistas del programa cumplan con esta Política.

6 Violación a la seguridad de la Información de Identificación Personal

La Oficina de Gerencia y Presupuesto (**OMB**, por sus siglas en inglés) identifica una violación de la seguridad de la información de identificación personal como un tipo de incidente. Un *incidente* es "un suceso que (1) pone en peligro real o inminente, sin autoridad legal, la integridad, confidencialidad o disponibilidad de información o un sistema de información; o (2) constituye una violación o amenaza inminente de violación de la ley, normas de seguridad, procedimientos de seguridad o normas de uso aceptable".[15]

Por otra parte, la OMB define una *violación* como "la pérdida de control, compromiso, divulgación no autorizada, adquisición no autorizada o un suceso similar en el que (1) una persona que no es el usuario autorizado tiene acceso o podría tener acceso a información de identificación personal o (2) un usuario autorizado tiene acceso o podría tener acceso a información de identificación personal para otros propósitos que no sean los autorizados".[16]

Los siguientes son ejemplos de incidentes que podrían conducir a una violación de la seguridad de la información de identificación personal:

- Pérdida, daño, hurto o disposición inadecuada de expedientes, documentos o equipo que contiene información de identificación personal;
- Enviar, por accidente o a propósito, archivos, documentos o informes que contienen información de identificación personal a una persona que no tiene autorización para ver, manejar o administrar dicha información;
- Enviar archivos o documentos que contienen información de identificación personal sin la protección adecuada (cifrado);
- Permitir que personas no autorizadas utilicen una computadora que contiene archivos y documentos con información de identificación personal;
- Discutir información de identificación personal en áreas públicas; y
- Cualquier situación que pueda comprometer la seguridad de la información de identificación personal (virus de computadora, "phishing", etc.).

La Ley Federal del Manejo de Seguridad de la Información de 2002 (**FISMA**, por sus siglas en inglés), 44 U.S.C. § 3541, *et seq*., según enmendada por la Ley Federal de Modernización de la Seguridad de la Información de 2014, Pub. L. 113-283, exige que todas las agencias federales desarrollen, documenten e implementen programas a nivel de toda la agencia para proteger sus sistemas de información y los datos que estos contienen, con el fin de respaldar las operaciones y los activos de la agencia, incluidos los provistos o administrados por otra agencia o contratista u otra fuente. FISMA aplica

[15] Memorando 17-12 de la OMB, emitido el 3 de enero de 2017, sobre Cómo prepararse y responder a una violación de información de identificación personal, https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/memoranda/2017/m-17-12_0.pdf
[16] Íd.

a todas las agencias del gobierno federal e incluye a las agencias estatales que administran programas federales.

Las alegaciones de violaciones a las medidas de protección de la información de identificación personal estarán sujetas a investigación y posibles medidas disciplinarias, en virtud de los requisitos de FISMA.

El incumplimiento con esta Política podría conllevar medidas disciplinarias por parte de Vivienda e imposición de sanciones por HUD.

6.1 Prevención de violaciones a la Información de Identificación Personal

Vivienda es responsable de velar por que los Programas CDBG-DR mantengan esta Política y supervisen, coordinen y faciliten los esfuerzos de cumplimiento. Vivienda se asegurará de que los empleados, subrecipientes y el personal de los Programas CDBG-DR sea instruido con respecto a la confidencialidad, no divulgación y protección de la información de identificación personal y las medidas contra las violaciones a la seguridad de la información.

6.1.1 Capacitación y concienciación

Vivienda garantiza que todos los empleados han recibido suficiente capacitación sobre el manejo y protección de la información de identificación personal, así como acerca de identificar y responder a incidentes de seguridad, lo que incluye, sin limitarse a esto, al personal y los empleados del Programa CDBG-DR que tienen acceso a información de identificación personal y a los sistemas que se utilizan para recopilar, administrar, transmitir o disponer de la información de identificación personal. Los talleres de capacitación deben hacer hincapié en la información provista en esta Política y cualquier otro documento guía, lo que incluye, por ejemplo:

- La importancia de proteger la confidencialidad de una persona;
- Identificar la información que debe protegerse;
- Protección de datos y expedientes;
- Almacenamiento adecuado de la información;
- Cómo evitar el intercambio inadecuado o no intencional de datos; y
- Cómo identificar y responder a incidentes de seguridad que involucran información de identificación personal.

6.2 Cómo reportar una violación a la seguridad de la Información de Identificación Personal

De conformidad con esta Política, toda sospecha o confirmación de alguna violación a la seguridad de la información de identificación personal, de cualquier manera o por cualquier medio, deberá reportarse a su supervisor lo antes posible y sin ningún retraso razonable. Por su parte, el supervisor es responsable de referir el incidente al Subsecretario de Vivienda. El hecho de no informar de inmediato un incidente puede socavar la habilidad de mitigar de inmediato la situación y de aplicar medidas preventivas y/o correctivas para proteger la información de identificación personal o

reducir el daño que el incidente podría causar a las personas. Se deben mantener registros y documentar la información y las acciones relacionadas con el incidente.

6.3 Cómo evaluar una violación a la seguridad de la Información de Identificación Personal

Al evaluar el tipo y la gravedad de una violación, Vivienda debe considerar tanto la intención como el destinatario. El acto de analizar la intención en una violación a la seguridad de la información de identificación personal, se refiere a determinar si la información se puso en peligro intencionalmente o de manera involuntaria, o si se desconoce cuál fue la intención. Vivienda también evaluará si se conoce o se desconoce quién fue el destinatario de la información de identificación personal divulgada, así como la honradez de dicho destinatario, si se conoce quién es el destinatario.[17] Esta evaluación proporcionará un marco de referencia sobre el riesgo relacionado con la posible o confirmada violación a la seguridad de la información de identificación personal.

Los incidentes relacionados con la privacidad pueden clasificarse como de impacto bajo, moderado o alto con base en la gravedad del incidente. Los factores que se toman en cuenta para llevar a cabo esta evaluación son:

- El carácter delicado de la información de identificación personal involucrada;
- La cantidad de personas afectadas; y
- El daño que puede causar o que ha causado el incidente.

Un incidente se clasifica como de bajo impacto cuando ocurre un uso, divulgación o disposición no autorizada o no ética de la información que podría tener un efecto adverso limitado sobre las operaciones organizacionales o las personas afectadas. Un incidente de impacto moderado se define como la divulgación de información que podría tener un efecto adverso. No obstante, en un incidente de alto impacto, el efecto causado por el incidente es un efecto adverso grave.[18] Un incidente que involucra información de identificación personal sensitiva se clasificará como un incidente de alto impacto.

Los siguientes son ejemplos de posibles incidentes que involucran una violación de la seguridad de la información de identificación personal:

- Pérdida de equipo;
- Intrusión a la seguridad;
- Divulgación no autorizada;
- Adquisiciones no autorizadas; y
- Acceso no autorizado.

[17] Memorando 17-12 de la OMB, Cómo prepararse y responder a una violación de información de identificación personal, https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/memoranda/2017/m-17-12_0.pdf
[18] Plan de respuesta a una notificación de violación de HUD, https://www.hud.gov/sites/documents/INCIDENT_RESPONSE.PDF

La evaluación del incidente formará parte del informe de incidente, junto con una descripción del incidente. El informe debe incluir información sobre quién, cuál, cuándo y cómo:

¿Quién?	¿Quién fue el responsable del incidente? ¿Quién se vio afectado por el incidente?
¿Cuál?	¿Cuál es la información que se vio comprometida? ¿Cuál es el impacto de que dicha información se haya visto comprometida?
¿Cuándo?	¿Cuándo ocurrió el incidente? ¿Cuándo se detectó? ¿Cuándo se reportó?
¿Cómo?	¿Cómo se tuvo acceso a la información? ¿Cómo se detectó el incidente?

Aunque es fundamental documentar adecuadamente el incidente, es importante señalar que el proceso de reportar el incidente no debe retrasar la implementación de las medidas necesarias para mitigar y responder a un incidente y tampoco se deben postergar estas medidas para obtener información adicional.

6.4 Cómo mitigar el riesgo de una violación a la seguridad de la Información de Identificación Personal

Vivienda está preparado para actuar de inmediato cuando ocurre una violación a la seguridad de la información de identificación personal, para reducir el posible riesgo que podrían enfrentar las personas afectadas. Una vez que se ha realizado una evaluación completa del riesgo, el siguiente paso es aplicar las medidas adecuadas para mitigar el posible daño que la violación, potencial o confirmada, de información de identificación personal podría causar las personas. Debido a que cada incidente de violación de información de identificación personal se basa en hechos específicos, las medidas requeridas para mitigar los posibles daños dependerán de cada caso. Al considerar la necesidad de mitigar los daños, se deben considerar los siguientes factores:

- Los daños ocurridos, si alguno;
- La naturaleza del daño;
- La cantidad y gravedad de los daños;
- El tipo de datos revelados;
- La razón de la divulgación; y
- Si, en efecto, es posible mitigar los daños.

Las medidas de mitigación pueden incluir contramedidas, orientación y/o servicios. Las contramedidas deben ponerse en marcha de inmediato e incluyen, por ejemplo, cancelar los nombres de usuario y contraseñas de las cuentas afectadas o colocar una alerta en una base de datos que contiene información de identificación personal que podría estar afectada. Se deberán implementar medidas de orientación, tales como explicar a las personas cómo pueden obtener más información sobre la violación y las medidas que, por su parte, pueden tomar. Aunque las medidas de servicio, por ejemplo, la recuperación de la identidad o los servicios de monitoreo de crédito, no siempre están disponibles para mitigar los posibles daños, se puede ofrecer información, orientación o métodos para adquirir dichos servicios.

6.5 Notificación de las violaciones a la seguridad de la Información de Identificación Personal

Se debe notificar a todas las partes afectadas por una violación a la seguridad de la información de identificación personal en un plazo de **cuarenta y cinco (45) días**[19], a partir de la determinación de que se ha cometido una violación y de que se haya identificado debidamente a las partes afectadas. Al notificar a una parte afectada, se debe tomar en cuenta el momento, la fuente del aviso, el contenido y el método de notificación.[20] Vivienda es responsable de notificar a las partes afectadas por la violación. La comunicación debe incluir una descripción que incluya las fechas, el tipo de información de identificación personal involucrada, las medidas que el Programa CDBG-DR de Vivienda ha tomado para mitigar los daños causados por la violación, las medidas que tendrían que tomar para protegerse más contra la violación, así como establecer una persona de contacto junto con su información.

6.5.1 Las violaciones a la seguridad de los bancos de información y la notificación a los ciudadanos

La Ley de Información al Ciudadano sobre Seguridad de Bancos de Información de Puerto Rico, Ley 111-2005, según enmendada, 10 LPRA § 4051, *et seq.*, dispone que toda entidad[21] propietaria o custodia de un banco de información que incluya información[22] personal de ciudadanos residentes en Puerto Rico, deberá notificar a dichos ciudadanos de cualquier violación de la seguridad del sistema, cuando los bancos de datos cuya seguridad fue violada contuvieran, en todo o en parte, de su archivo de información personal y la misma no estuviera protegida con claves criptográficas más allá de una contraseña. La notificación de dicha violación se enviará de forma clara y conspicua y deberá describir, en términos generales, la violación de la seguridad y la información involucrada. Esta notificación incluirá un número de teléfono del Programa CDBG-DR de Vivienda o información sobre un sitio web donde las personas puedan obtener más información o asistencia. La notificación se enviará por escrito a todos los posibles afectados a través del correo regular o por correo electrónico autenticado de conformidad con lo establecido en la Ley de Transacciones Electrónicas de Puerto Rico, Ley 148-2006, según enmendada, 10 LPRA § 4081. Si el costo de notificar o identificar a todas las partes afectadas resulta demasiado oneroso, o si el costo supera los cien mil dólares ($100,000) o las partes afectadas son más de cien mil (100,000), la notificación deberá hacerse:

---

[19] El término de cuarenta y cinco 45 días es un plazo establecido por HUD, en su Plan de respuesta a una notificación de violación, https://www.hud.gov/sites/documents/INCIDENT_RESPONSE.PDF

[20] Plan de respuesta a una notificación de violación de HUD, https://www.hud.gov/sites/documents/INCIDENT_RESPONSE.PDF

[21] Para propósitos de esta ley, la definición de entidad incluye toda agencia y toda instrumentalidad u organismo gubernamental de cualquiera de las tres ramas del gobierno, así como toda corporación pública, compañía u organización privada autorizada a realizar negocios u operar en Puerto Rico. 10 LPRA § 4051(d).

[22] Para propósitos de esta ley, la definición de información personal incluye el nombre o primera inicial y el apellido paterno de una persona, combinado con cualquiera de los siguientes datos: número de Seguro Social, licencia de conducir, tarjeta electoral o cualquier otro número de identificación personal, números de cuentas bancarias o cualquier otro tipo de información financiera, nombres de usuario y claves de acceso a sistemas informáticos públicos o privados, información médica protegida por la Ley HIPAA, información contributiva y evaluaciones laborales. 10 LPRA § 4051(d).

1. Mediante la publicación de un anuncio al respecto en el lugar de hacer negocios de la entidad, en la página electrónica de la entidad, si alguna, y dentro de cualquier volante informativo que publique y envíe a través de listas de correo, tanto postales como electrónicas; y,
2. Al emitir una comunicación al respecto a los medios de prensa, que informe de la situación y provea información sobre cómo comunicarse con la entidad para darle mayor seguimiento. Cuando la información sea de relevancia en un sector específico (profesional o comercial), se podrá efectuar este anuncio a través de las publicaciones o la programación de mayor circulación orientada a ese sector. 10 LPRA § 4053.

6.6 Requisitos para Contratistas, Subrecipientes y otros Socios

Los contratistas, subrecipientes y socios deben asegurarse de que todos los procedimientos establecidos en sus Políticas acerca de la información de identificación personal incluyan los procesos correspondientes de capacitación, administración y respuesta a violaciones. Se sugiere exigir que los contratistas reciban capacitación en cuanto a las políticas sobre violaciones a la seguridad de la información de identificación personal (que incluirán la identificación, informe, mitigación y prevención de las violaciones); cuenten con sistemas adecuados y tengan la capacidad de determinar el acceso a la información (cuándo, dónde y por quién) para monitorear la seguridad de la información de identificación personal, y permitan la realización de inspecciones o investigaciones para garantizar el cumplimiento con esta Política. Estas medidas deben permitir que Vivienda responda adecuadamente y a tiempo a cualquier violación real o potencial. Como parte de las medidas de respuesta a violaciones a la seguridad de la información de identificación personal, los contratistas, subrecipientes y socios deberán cooperar e intercambiar información con Vivienda para informar y manejar de forma efectiva las violaciones reales o potenciales. Al realizar este intercambio de información, se implementarán las mejores prácticas de seguridad.

7 Mejores Prácticas Recomendadas para el Manejo Seguro de la Información de Identificación Personal

Vivienda administra un alto volumen de información de identificación personal en la implementación de los programas CDBG-DR. Se espera que su personal, subrecipientes y agencias asociadas, así como el personal de estas, protejan la información que los solicitantes de los programas les han confiado. Existen varias estrategias y actividades que se deben implementar al administrar y manejar la información de identificación personal. En esta sección se incluye una lista, no exhaustiva, de las mejores prácticas sugeridas.

7.1 Prácticas generales

- Limitar la recopilación, acceso, uso y divulgación de información personal a las funciones legítimas del trabajo o las razones permitidas por ley;

- Proteger la información personal cuando esté en posesión de la persona;
- Seguir métodos adecuados para la eliminación de documentos que contienen información de identificación personal; y
- Informar inmediatamente los actos o incidentes sospechados o confirmados de violaciones a la privacidad.

7.2 Identificaciones de usuario y contraseñas

- Las identificaciones de usuario y contraseñas son para uso personal y no se deberán compartir.
- Esta información se considera privada y confidencial y debe tratarse como tal.
- Las contraseñas deben interpretarse como contraseñas sólidas que contienen un mínimo de ocho (8) caracteres con una combinación de letras mayúsculas y minúsculas, números y caracteres especiales.[23]
- No deben ser fáciles de adivinar.
- Las contraseñas deben cambiarse con regularidad, según lo determine la Política de Seguridad Informática.
- No se debe permitir que ni las identificaciones de usuario ni las contraseñas se incluyan en un proceso automatizado de inicio de sesión o se guarden en el navegador.

7.3 Expedientes

- Los expedientes no deberán ser removidos de la oficina sin consentimiento previo.
- El supervisor del empleado/contratista debe otorgar el consentimiento, por escrito, para remover un expediente de la oficina.
- Los expedientes se deben mantener en gabinetes de archivo.
- Los gabinetes de archivo deben estar cerrados con llave cuando no estén en uso. Solo los empleados o contratistas autorizados tendrán una copia de las llaves del gabinete.
- Los expedientes o documentos que salgan de la oficina deberán estar asegurados y asignados a una persona específica. Debe llevarse un registro por escrito de quién se encuentra en control físico o electrónico de los expedientes y documentos.
- Los expedientes inactivos deberán estar sujetos a la política correspondiente sobre retención de expedientes.
- Todo documento duplicado que contenga información confidencial o sensible deberá triturarse.

7.4 Computadoras

- Se deben establecer barreras y controles adecuados entre el personal no autorizado y los documentos o pantallas de computadora que contengan información confidencial o sensitiva.

[23] Normas de seguridad en la tecnología informática del Programa CDBG-DR del Departamento de la Vivienda de Puerto Rico, 23 de agosto de 2019, página 11.

- Las pantallas de las computadoras deben colocarse de manera que el personal no autorizado no pueda tener acceso ni leer la pantalla.
- La información almacenada en las computadoras debe utilizar un sistema seguro.
- La información confidencial o sensitiva no debe enviarse por correo electrónico a ninguna persona que no se encuentre en las instalaciones del lugar de trabajo.
- Las computadoras no deberán dejarse desatendidas sin bloquear el acceso o desconectarse del sistema.

7.5 Protección antivirus

- La protección antivirus es obligatoria para todos los equipos, estaciones de trabajo y servidores que se utilizan para manejar la información de identificación personal.
- Es de vital importancia que el programa o software antivirus se mantenga actualizado en todas las computadoras.

7.6 Violaciones a la seguridad de la Información de Identificación Personal

- El empleado o contratista deberá notificar de inmediato toda violación real o potencial de la seguridad de la información de identificación personal o de esta Política a su supervisor en Vivienda o en la oficina de su gerente general.
- Reportar, evaluar, mitigar y notificar las violaciones a la seguridad de la información de identificación personal según se establece en esta Política y en cualquier otro documento guía que se haya desarrollado.
- Las medidas incluyen, entre otras, el manejo de riesgos, establecer un equipo de respuesta, identificar la causa, identificar las medidas de mitigación y las medidas de seguimiento para evitar futuros incidentes.

8 Aprobación

Esta política será efectiva inmediatamente luego de su aprobación y deroga cualquier versión anterior. Este documento es una traducción de la versión en inglés, por lo que, de haber alguna inconsistencia entre ambas versiones, la versión en inglés prevalecerá. Véase la versión en inglés para constatar su firma de aprobación.

FIN DE LA POLÍTICA.