CDBG-DR/MIT

Política sobre Información de Identificación Personal, Confidencialidad y No Divulgación

DEPARTAMENTO DE LA VIVIENDA
GOBIERNO DE PUERTO RICO

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

7 de abril de 2025
V.3

Esta página se dejó en blanco intencionalmente.

DEPARTAMENTO DE LA VIVIENDA DE PUERTO RICO

PROGRAMAS CDBG-DR/MIT

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**	**Traducción de la versión original en inglés.**
2	**17 de septiembre de 2020**	**Se añadió información en varias secciones a través de todo el documento a los efectos de agregar información recopilada del Informe OIG de HUD: *HUD PII Records Protection and Management, 2019-OE-0002a* del 25 de junio de 2020, así como otras referencias de HUD. Todas las ediciones aparecen resaltadas en color gris.**
3	**7 de abril de 2025**	**Se realizaron ediciones a lo largo del documento para incorporar referencias al Programa CDBG-MIT, reorganizar el contenido, actualizar definiciones conforme al Código de Regulaciones Federales e integrar la Ley de Ciberseguridad del Estado Libre Asociado de Puerto Rico, Ley Núm. 40-2024. Asimismo, se revisaron los procedimientos y regulaciones. Todos los cambios están resaltados en color gris.**

Índice

1 Introducción

El Departamento de la Vivienda de Puerto Rico (**Vivienda**), como administrador de los fondos, está comprometido con el manejo responsable de los fondos de la Subvención en Bloque para Desarrollo Comunitario - Recuperación ante Desastres (**CDBG-DR**, por sus siglas en inglés) y de la Subvención en Bloque para Desarrollo Comunitario - Mitigación (**CDBG-MIT**, por sus siglas en inglés). Como parte de su compromiso, Vivienda prioriza la protección de la privacidad de las partes interesadas. Durante la administración de los programas CDBG-DR/MIT, el personal puede estar expuesto o tener acceso a Información de Identificación Personal (**PII**, por sus siglas en inglés). Para proteger esta información, se deben tomar las medidas adecuadas para garantizar que los documentos que incluyen PII se manejen y sean almacenados 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, recipientes y subrecipientes de los Programas CDBG-DR/MIT de Vivienda. Esta política garantiza que la PII 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 garantizar la protección de la información confidencial y/o sensitiva en todos los procesos de Vivienda y del Programa CDBG-DR/MIT. Al resaltar la estricta observancia de las medidas de confidencialidad, esta política fomenta la confianza y credibilidad dentro del Programa CDBG-DR/MIT de Vivienda. Además, contribuye a resguardar la PII de los participantes, empleados, subrecipientes y contratistas frente a posibles violaciones de la seguridad de la información.

4 Definiciones

Confidencialidad: Preservar las restricciones autorizadas sobre el acceso y la divulgación, incluyendo la protección de la privacidad personal y la información confidencial.[1]

Contratista: Un proveedor o suplidor, según corresponda, 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 Vivienda y Desarrollo Urbano de los Estados Unidos.

Información de Identificación Personal (PII, por sus siglas en inglés): Información que puede ser utilizada para distinguir o rastrear la identidad de una persona, ya sea por sí sola o cuando se combina con otra información personal o identificación que esté vinculada o pueda vincularse a un individuo específico. Algunos datos de PII están disponibles en fuentes públicas, como guías telefónicas, sitios web y listados universitarios. La definición de PII no está limitada a una sola categoría de información o tecnología; en cambio, requiere una evaluación caso a caso del riesgo específico de que una persona pueda ser identificada. La información que no es de identificación personal puede convertirse en PII cuando se hace pública información adicional, en cualquier medio y de cualquier fuente, que -al combinarse con otra información disponible- podría utilizarse para identificar a una persona.[2]

Información de Identificación Personal Protegida (PII Protegida): Para propósitos de esta política, la PII Protegida se refiere a la PII que, cuando se presenta junto con PII Sensitiva, requiere medidas de protección más rigurosas para proteger la privacidad del individuo y prevenir el acceso o la divulgación no autorizados.[3]

---

[1] 44 U.S.C. § 3552.

[2] 2 C.F.R. §200.1.

[3] Anteriormente, la PII Protegida, según lo establecido en 2 C.F.R. Parte 200, se definía como el nombre o la inicial del nombre junto con el apellido de una persona, cuando se combinaba con información sensible, como números de Seguro Social, números de pasaporte, registros financieros, registros médicos o datos biométricos. Esta definición reconocía que la combinación de estos elementos aumentaba el riesgo de perjuicio en caso de divulgación. Bajo la versión revisada de 2 C.F.R. §200.1, la PII Protegida ahora se define como "PII, excepto aquella que deba ser divulgada

Información de Identificación Personal Sensitiva (PII Sensitiva): La información de identificación personal que, en caso de pérdida, vulneración o divulgación no autorizada, podría causar un perjuicio significativo a una persona. Algunos ejemplos de PII Sensitiva incluyen números de seguro social o de licencia de conducir, registros médicos y números de cuentas financieras.[4] La PII Sensitiva puede incluir información independiente o información combinada con otro identificador.

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/MIT.

Subrecipiente: Una entidad que recibe una subadjudicación de una entidad intermediaria para llevar a cabo parte de subvención federal. El término no incluye a un beneficiario o participante.

Violación a la seguridad de la información: Para propósitos de esta política, el término se utiliza para incluir la pérdida de control, la vulneración, la divulgación no autorizada, la adquisición no autorizada, el acceso no autorizado o cualquier término similar que haga referencia a situaciones en las que personas distintas a los usuarios autorizados, y para un propósito no autorizado, tengan acceso o puedan tener acceso a información de identificación personal, ya sea en formato físico o electrónico.[5]

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

---

por ley." Sin embargo, para garantizar claridad, esta política define la PII Protegida como aquella PII, que cuando se presenta junto con PII Sensitiva requiere medidas de protección más rigurosas.

[4] HUD, Guía de Desarrollo de Capacidades para la Protección de PII: Orientación sobre la Protección de Información Privada, abril 2015, https://files.hudexchange.info/resources/documents/Housing-Counseling-Protecting-PII-Capacity-Building-Guidance-Protecting-Privacy-Information.pdf.

[5] OMB, Memorando 07-16, sobre Protección y Respuesta ante una Violación de Información de Identificación Personal, 22 de mayo de 2007, https://obamawhitehouse.archives.gov/sites/default/files/omb/assets/omb/memoranda/fy2007/m07-16.pdf.

5 Información de Identificación Personal

Para implementar los Programas CDBG-DR/MIT, Vivienda necesita recopilar, mantener, utilizar, recuperar y difundir información relacionada con las personas que solicitan asistencia. Debido a la naturaleza de los programas, los expedientes de los Solicitantes pueden incluir datos sensitivos como información sobre sus ingresos, seguros, números de cuentas bancarias, contraseñas, Números de Identificación Personal (**PIN**, por sus siglas en inglés), informes de inspección de viviendas y anotaciones sobre diversos tipos de asistencia. Parte de la información incluida en los expedientes de los Solicitantes, sino toda, se considera PII.

La información de identificación personal incluye cualquier 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 esté 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 intencionalmente amplia y no se limita en una sola categoría de información o tecnología. En cambio, requiere de un análisis caso a caso para determinar si ciertos datos, combinados con otros detalles disponibles públicamente (independientemente de la fuente o el medio), podrían identificar a una persona.

Dado el amplio alcance de la definición de PII, el contexto juega un papel fundamental en la determinación del nivel adecuado de medidas de protección a aplicar. Sin embargo, al manejar PII, es recomendable adoptar un enfoque prudente para garantizar el más alto nivel de protección.

5.1 PII Sensitiva y PII Protegida

La información Identificación Personal Sensitiva (**PII Sensitiva**, por sus siglas en inglés) se refiere a aquella información que, si se pierde, se ve comprometida o se divulga sin autorización, podría perjudicar sustancialmente a una persona. Debido al alto riesgo asociado con su acceso o exposición no autorizada, la PII Sensitiva requiere protocolos de manejo reforzados y medidas de seguridad más estrictas.

Ciertos tipos de PII son inherentemente sensitivos como elementos de datos independientes, tales como el número de Seguro Social (**SSN**, por sus siglas en inglés), la licencia de conducir o el número de identificación estatal. Además, otros elementos

de datos—como el estatus de ciudadanía o inmigración, información médica, afiliación étnica o religiosa, orientación sexual o detalles sobre el estilo de vida—se convierten en PII Sensitiva cuando están asociados con la identidad de una persona, ya sea de manera directa o indirecta. Cuando la PII se vincula con PII Sensitiva, también debe protegerse adecuadamente, lo que lleva a su clasificación como Información de Identificación Personal Protegida (**PII Protegida**, por sus siglas en inglés).

Para propósitos de esta política, todas las salvaguardas y medidas de protección se aplicarán de manera integral tanto a la PII Sensitiva y Protegida. Este enfoque garantiza un nivel de protección coherente y exhaustivo, reconociendo los mayores riesgos que surgen cuando los elementos de datos están vinculados. Al aplicar estas rigurosas medidas de seguridad, la política busca garantizar la confidencialidad, integridad y seguridad de esta información.

5.2 Acceso y Manejo de PII Sensitiva y Protegida

De acuerdo con el 2 C.F.R. 200.303(e), como parte del control interno al manejar fondos de adjudicaciones federales, el personal de Vivienda, sus subrecipientes y contratistas deben "[t]omar medidas razonables para proteger la información de identificación personal protegida y demás información que la agencia federal adjudicadora o la entidad intermediaria designen como sensitiva o que la entidad no federal considere sensitiva de acuerdo con las leyes federales, estatales, locales y tribales aplicables, relacionadas con la privacidad y las obligaciones de confidencialidad".

En la implementación, manejo y ejecución de los Programas CDBG-DR/MIT, el personal de Vivienda, sus subrecipientes, contratistas y agencias asociadas recopilarán, utilizarán, procesarán, almacenarán, difundirán, y tendrán acceso a una cantidad significativa de información personal de los solicitantes. Todas las personas que tengan acceso a información confidencial de los solicitantes son responsables de la protección de la información de contraseñas, equipos, expedientes de casos y canales de comunicación.

Para garantizar el cumplimiento de estos requisitos, Vivienda ha implementado salvaguardas, medidas de protección y mejores prácticas para la protección de la PII

Sensitiva y Protegida obtenida a través de la implementación, gestión y ejecución de los Programas CDBG-DR/MIT.

5.2.1 Confidencialidad y No divulgación

El derecho a la privacidad y al control sobre la información personal de los solicitantes está consagrado en la Constitución del Estado Libre Asociado de Puerto Rico. Como parte de esta protección constitucional, es responsabilidad del Estado salvaguardar el derecho de las personas a su dignidad, intimidad e integridad personal.[6]

Las personas con acceso autorizado a la información confidencial de los solicitantes deben ser instruidas sobre el derecho a la privacidad y la protección de la información personal, conforme a lo dispuesto en el Artículo 173 del Código Penal de Puerto Rico de 2012, 33 LPRA § 5239 *et seq*., el cual 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[7] y 172[8] del Código, o que ofrezca o solicite dicha distribución o acceso, estará sujeta a una pena fija de prisión de tres (3) años. Si la persona condenada es una entidad legal, estará sujeta a una multa de hasta diez mil dólares ($10,000).

Los subrecipientes, contratistas y subcontratistas de los Programas CDBG-DR/MIT de Vivienda deben cumplir con la cláusula de confidencialidad y no divulgación establecida en sus contratos o acuerdos de subrecipiente. Además, el personal de Vivienda, los subrecipientes y contratistas solo deben acceder a información confidencial o sensitiva que sea relevante para el programa al que están asignados,

[6] CONST. P.R. Art. II, § 8.

[7] El Artículo 171, 33 LPRA § 5237, 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.

[8] El artículo 172, 33 LPRA § 5238, 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.

salvo aquellos empleados que, por la naturaleza de su cargo, deban tener acceso a múltiples programas.

Todos los empleados de Vivienda y de los subrecipientess, contratistas, agencias asociadas y demás personal del Programa con acceso a información confidencial o sensitiva deben firmar un Acuerdo de Confidencialidad y No Divulgación. Este acuerdo formará parte del expediente del empleado junto con la constancia de recibo de esta Política.

Las excepciones a la limitación de acceso a información confidencial o sensitiva aplican cuando el acceso es requerido por agencias de monitoreo o supervisión y su personal, ya sean federales o locales. No obstante, el personal encargado del monitoreo o supervisión que tenga acceso a expedientes, documentos, computadoras y otros dispositivos que contengan PII Sensitiva y Protegida deberá cumplir con los mismos estándares estrictos de seguridad y confidencialidad aplicables al personal de los Programas CDBG-DR/MIT. Cualquier información divulgada debe limitarse estrictamente al programa o área específica bajo revisión. El acceso a dicha información debe ser cuidadosamente supervisado, y cualquier acceso electrónico debe estar sujeto a roles y privilegios personalizados que permitan rastrear y mantener un registro de todos los datos consultados.

5.2.1.1 Ley de Ciberseguridad del Estado Libre Asociado de Puerto Rico

La Ley de Ciberseguridad del Estado Libre Asociado de Puerto Rico, Ley Núm. 40-2024, 3 LPRA § 10121, establece la política pública para la protección de la información y la infraestructura gubernamental, garantizando su confidencialidad, integridad y disponibilidad a lo largo de su ciclo de vida, lo que incluye su almacenamiento, transmisión y procesamiento.

Esta ley es aplicable Vivienda, sus empleados, subrecipientes, contratistas y cualquier persona natural o jurídica que realice negocios o celebre contratos con el gobierno. Vivienda está comprometido con el cumplimiento de los estándares y principios mínimos de ciberseguridad establecidos en esta ley, los cuales incluyen, pero no se limitan a:

- Establecer mecanismos de control para detener tráfico de internet inapropiado e implementar una política de seguridad que restrinja el acceso a sitios web

con programas malignos ("*malware*"), suplantación de identidad u obtener datos de la identidad de usuario ("*phishing*") *y* otras amenazas identificadas, salvo cuando el acceso sea necesario para el cumplimiento de funciones oficiales;

- Establecer controles de seguridad en capas para reforzar la confidencialidad, integridad y autorización de la información;
- Desarrollar políticas de uso adecuado de equipos y sistemas de información, además de implementar controles administrativos y técnicos para regular el acceso a redes internas y externas;
- Adoptar controles administrativos que exijan el cifrado de datos basado en las recomendaciones del Instituto Nacional de Estándares y Tecnología (**NIST**, por sus siglas en inglés) para mejorar la confidencialidad e integridad de la data en transporte y en almacén. Establecer mecanismos técnicos para forzar las políticas establecidas;
- Establecer que las conexiones remotas a la red del gobierno se realizarán únicamente a través de una red privada virtual (**VPN**, por sus siglas en inglés) o cualquier otro programa de red privada virtual que el gobierno contrate exclusivamente para uso oficial cuando las tareas relacionadas con el trabajo sean necesarias;
- Todo software o aplicación desarrollado o utilizado por Vivienda o sus proveedores contratados para atender a los ciudadanos o facilitar operaciones internas debe cumplir con los estándares mínimos de seguridad.
- Establecer un mecanismo de clasificación de datos basado en su criticalidad para el gobierno y los ciudadanos, después de esta clasificación se establece el uso de autenticación multifactorial (**MFA**, por sus siglas en inglés) para todo usuario;
- Incluir en los contratos con proveedores de servicios medidas para proteger activos sensibles y exigir el cumplimiento de la Ley Federal de Administración de Seguridad de la Información de 2002 (**FISMA**, por sus siglas en inglés), 44 U.S.C. § 3541, *et seq;*
- Los proveedores de servicios contratados de tecnología de la información y comunicaciones compartirán información y notificarán en un término no mayor de cuarenta y ocho (48) horas al *Puerto Rico Innovation and Technology*

Service (**PRITS**) y a Vivienda cuando descubran un incidente de seguridad cibernética o un incidente potencial que pueda poner en Riesgo los datos, productos de "*software"*, "*firmware"* o los servicios confidenciales del Gobierno o de cualquier persona natural o jurídica;

- Garantizar que los sistemas de Tecnología de Información (**IT,** por sus siglas en inglés) gubernamentales se utilicen exclusivamente para propósitos autorizados, con acceso basado en roles;
- Las instalaciones y activos de procesamiento de información deberán estar alojados en áreas seguras, no rotuladas, protegidas con un perímetro de seguridad apropiado y controles para evitar el acceso no autorizado y daños y deberán contar con un generador eléctrico para evitar fallas en caso de problemas con el servicio eléctrico, como parte de un protocolo de contingencia;
- Garantizar que la información confidencial, incluida la PII, no quedará expuesta ni desprotegida en ninguna circunstancia. Deberá estar encriptada en todos sus estados (es decir, en tránsito y en reposo);
- Establecer y mantener un programa de educación en ciberseguridad para el personal y los proveedores de servicios;
- Desarrollar e integrar planes de respaldo y recuperación de datos para velar por la continuidad de las operaciones, considerando sistemas mantenidos localmente y los sistemas mantenidos por suplidores o terceros tipo "*cloud*";
- Cumplir con cualquier estándar adicional de ciberseguridad publicado por PRITS.

5.2.2 Terminación y Acceso a la Información

El proceso de terminación de empleo ("*offboarding*") deberá involucrar a la división de Recursos Humanos, Operaciones, Sistemas de Información (**IT**, por sus siglas en inglés), y cualquier otra área pertinente a la que el empleado haya tenido acceso a expedientes, discos de almacenamiento de datos, aplicaciones o cualquier otro método de manejo de información.

Durante el proceso de terminación de empleo, las áreas correspondientes trabajarán de manera coordinada para identificar la información, discos o aplicaciones a los que el empleado haya tenido acceso, con el fin de desactivar todas las credenciales y

privilegios de acceso que le fueron asignados. Es responsabilidad del supervisor del empleado o el director de la división de notificar al área de IT y solicitar formalmente la eliminación de todos los derechos de acceso. Además, si el dispositivo asignado al empleado o su teléfono móvil contienen aplicaciones que sincronizan la información de correos electrónicos, contactos, calendarios y discos de almacenamiento remoto de datos, estos deberán verificados y desactivados de inmediato.

El proceso de terminación debe garantizar la ejecución de las siguientes acciones:

- Reforzar la importancia del mantenimiento de la confidencialidad;
- Recuperar cualquier información que el empleado tenga en su posesión;
- Recuperar todos los aparatos electrónicos, fuera de la oficina, 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

El uso de información se limitará a garantizar el cumplimiento de los requisitos del Programa, las regulaciones de HUD y las normativas federales; reducir 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 de los Programas CDBG-DR/MIT de Vivienda. El Formulario de Consentimiento debe detallar la información a ser compartida y debe ser firmado y fechado por la parte afectada.

Algunos programas CDBG-DR/MIT permiten a los Solicitantes designar a un tercero para obtener información sobre su solicitud al Programa. Este tercero se conoce como Designado de Comunicación. El Designado de Comunicación actúa como punto de contacto para el Solicitante, pero no es un Poder notarial. El Designado de Comunicación puede recibir y proveer información al Programa en nombre del Solicitante. No obstante, no puede firmar ningún documento ni establecer ningún acuerdo, a menos que no le haya otorgado la autoridad mediante un Poder notarial.

5.2.4 Recopilación de PII

La recopilación de PII Sensitiva y Protegida debe limitarse estrictamente a lo necesario para la implementación y gestión efectiva de los Programas CDBG-DR/MIT y no debe ser recopilada ni almacenada sin la debida autorización. Cuando la PII se utilice para determinar los derechos, beneficios o privilegios de una persona solicitante, dicha información debe obtenerse directamente del individuo, siempre que sea posible.

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, municipios, corporaciones públicas y sus contratistas, dentro de parámetros 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 Núm. 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 Núm. 207- 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. Los empleados pueden renunciar voluntariamente y por escrito a las protecciones de esta ley, pero esta renuncia no puede imponerse como condición de empleo.[9] Si un documento que contiene el número de Seguro Social de un trabajador debe hacerse público y este

[9] Las exenciones a la Ley Núm. 27-2006 aplican cuando el uso de un número de Seguro Social es legalmente requerido, autorizado o regulado por leyes o regulaciones federales. Asimismo, la ley no aplica cuando el número se utiliza para verificación de identidad, contribuciones fiscales, contratación o fines de nómina, siempre que el empleador implemente medidas de seguridad adecuadas para proteger su confidencialidad.

número no es necesario para el propósito del documento, el número deberá redactarse total o parcialmente para garantizar que sea ilegible.

La 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 Núm. 243-2006, según enmendada, 29 LPRA § 621(b), autoriza a las entidades gubernamentales, incluyendo agencias, departamentos, instrumentalidades del Estado Libre Asociado, las ramas Ejecutiva, Legislativa y Judicial, municipios, corporaciones públicas y sus contratistas, a recopilar números de Seguro Social para transacciones oficiales. Estos números pueden utilizarse para verificar identidad, cotejar registros internos y facilitar el intercambio de información. No obstante, cualquier entidad que solicite el número de Seguro Social de un ciudadano debe divulgar la autoridad legal que respalda la solicitud, el propósito previsto y si proporcionar el número es obligatorio o voluntario.

5.2.5 Acuerdos de Intercambio de Información

Como parte de los esfuerzos para recuperación y mitigación de desastres, Vivienda trabaja con las agencias federales y locales, socios y subrecipientes para compartir información, la cual, en muchas ocasiones, incluye PII Sensitiva y Protegida. Con el fin de imponer directrices claras, Vivienda ha establecido acuerdos para el intercambio de datos e información, también conocidos como Acuerdo de Intercambio y Acceso de Información (**ISAA**, por sus siglas en inglés). Estos ISAA definen las responsabilidades de las partes para proteger, manejar y compartir la PII.

Como parte de dichos esfuerzos, Vivienda suscribió un ISAA con la Agencia Federal para el Manejo de Emergencias (**FEMA,** por sus siglas en inglés). Mediante una enmienda al ISAA[10] original, FEMA permitió a Vivienda compartir información de identificación personal con sus contratistas. Este acuerdo, al igual que otros acuerdos de intercambio de información, puede sufrir enmiendas cada cierto tiempo, así como de prórrogas, para ampliar su período de vigencia. De acuerdo con DHS/FEMA 008 – Sistema de Registros de Archivos de Asistencia para Recuperación ante Desastres

[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.

("*Disaster Recovery Assistance Files System of Records*")[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.

Estos ISAA deben incluir, 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.
- 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/MIT.
- 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 manejan o tienen acceso a la información de identificación personal en cuanto a la naturaleza confidencial y las consecuencias legales que podrían enfrentar por el mal manejo de información.
- Medidas de seguridad técnicas, físicas y administrativas para proteger la información de identificación personal.
- Cumplimiento con los requisitos y regulaciones incluidas en el 2 C.F.R. Parte 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.

[11] DHS/FEMA 008 – Disaster Recovery Assistance Files System of Records [Sistema de Registros de Archivos de Asistencia para Recuperación ante Desastres], 78 FR 25283 (Apr. 30, 2013). El documento está disponible en: https://www.govinfo.gov/content/pkg/FR-2013-04-30/html/2013-10173.htm.

    - 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 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.

Es fundamental destacar que estos datos están protegidos bajo la Ley de Privacidad de 1974, 5 U.S.C. § 552a, *et seq*. Aunque la Ley de Privacidad no aplica a Puerto Rico ni a sus agencias, Vivienda, como recipiente de fondos de HUD, debe cumplir con los requisitos para manejo y protección de los datos recibidos de fuentes federales. Por lo tanto, Vivienda es responsable de gestionar el acceso a estos datos y debe:

- Solicitar los datos solo cuando sea necesario, basado en los requisitos específicos del programa descritos en el Plan de Acción aprobado.
- Limitar el acceso a Usuarios Autorizados, quienes deben cumplir con los requisitos de uso de datos especificados en el ISAA, reconocer sus responsabilidades bajo la Ley de Privacidad y FISMA, y ser informados sobre las sanciones civiles y penales por incumplimiento.
- Garantizar que los Usuarios Autorizados reciban capacitación sobre seguridad de la información y protección de la privacidad, de acuerdo con el ISAA, la Ley de Privacidad y FISMA.
- Realizar evaluaciones de riesgo y vulneración de datos para determinar si es necesario notificar al HUD o tomar medidas de remediación para las personas afectadas.

- Cifrar y almacenar de forma segura la PII de los solicitantes, ya sea en formato físico o electrónico, de manera que se prevenga cualquier acceso o uso no autorizado.

Además, Vivienda retendrá los datos recibidos de FEMA únicamente durante el período necesario para su procesamiento, generalmente hasta el cierre de la subvención. Cualquier dato de FEMA obtenido pero no utilizado deberá eliminarse una vez finalizado el procesamiento de la solicitud.

5.2.6 Métodos para la Transmisión

En ocasiones, puede ser necesario transmitir PII a individuos, agencias o personal autorizado del Programa. Sin embargo, dichas transmisiones deben limitarse a situaciones estrictamente esenciales y llevarse a cabo con las máximas precauciones para garantizar la seguridad de los datos. Todos los proveedores, vendedores, suplidores, contratistas, subcontratistas, consultores, socios y subrecipientes de los Programas CDBG-DR/MIT deberán redactar u omitir cualquier información confidencial o PII no esencial en las facturas y la documentación enviada por correo electrónico. En caso de ser imprescindible transmitir PII Sensitiva o PII Protegida, esta debe enviarse mediante aplicaciones web seguras o cifrarse antes de su envío por correo electrónico.

Se deben tomar medidas 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. El remitente se asegurará de que ninguna de las transmisiones esté almacenada en la memoria de la máquina de fax, que el fax esté ubicado en un área controlada y que todos los desechos de papel se eliminen adecuadamente. Al enviar por fax la información de identificación personal sensible, solo se utilizarán máquinas de fax controladas, no centros de recepción centrales.[12]

La PII Sensitiva y Protegida en documentos físicos no debe dejarse desatendida en escritorios, impresoras o en ninguna área accesible al personal no autorizado. Además, el personal debe asegurarse de que sus computadoras nunca queden

[12] Ver https://www.hud.gov/sites/documents/OHC_PII081214.PDF.

desatendidas de manera que puedan permitir el acceso no autorizado a dicha información.

Como se especifica en esta política, se deben tomar otras medidas para tratar la información como confidencial y proteger la transmisión de PII:

- Las conversaciones telefónicas en las que se discuta PII Sensitiva y Protegida deben realizarse únicamente después de confirmar que la persona con la que se habla está autorizada y ha sido informada de que la conversación incluirá este tipo de información.
- La PII Sensitiva y Protegida no debe incluirse en mensajes de voz en ningún medio de comunicación.
- No se debe incluir PII Sensitiva y Protegida en mensajes de voz, en ningún medio de comunicación.
- La PII Sensible y Protegida no debe discutirse en público ni en espacios compartidos donde personas no autorizadas pueden escuchar la conversación.

  Las reuniones en las que se discuta PII Sensitiva y Protegida deben realizarse en espacios seguros. Las minutas de estas reuniones deben considerarse como confidenciales si contienen información de identificación personal.[13] Se mantendrán registros de la fecha, hora, lugar, tema, presidente y asistentes de la reunión.[14]
- Los expedientes que contienen PII Sensitiva no deben ser retirados de las instalaciones donde la información está autorizada para ser almacenada y utilizada, a menos que se obtenga la aprobación de un supervisor primero.[15]
- Los sobres entre oficinas o translúcidos no se utilizarán para enviar PII Sensitiva y Protegida. En su lugar, se deben utilizar sobres opacos capaces de ser sellados.
- Al utilizar el Servicio Postal de EE.UU. para entregar PII Sensitiva y Protegida, los documentos deben estar doblemente envueltos (usando dos sobres, uno

[13] HUD, Guía para el desarrollo de la capacidad para proteger la información de identificación personal y la información privada, abril de 2015, https://www.hud.gov/sites/documents/OHC_PII042815.PDF.
[14] Ver https://www.hud.gov/sites/documents/OHC_PII081214.PDF
[15] *Id.*

dentro del otro) y marcar solo el sobre interno como confidencial con la declaración – Solo Para Ser Abierto Por El Destinatario.

5.2.7 Acceso Público a Registros

Según requerido por las leyes y reglamentos federales y estatales, la información pública contenida, almacenada o generada en entidades gubernamentales debe estar disponible para inspección pública, previa solicitud. Según lo dispuesto en 24 C.F.R. § 570.508, Vivienda debe proporcionar a los ciudadanos un acceso razonable a los registros relacionados con la utilización previa de los fondos CDBG, de conformidad con las leyes estatales y locales aplicables en materia de privacidad y confidencialidad. Para obtener más información sobre la accesibilidad de los registros por parte del público y el proceso completo de solicitud de información pública, consulte la Política sobre Manejo, Administración y Accesibilidad de Documentos, disponible en inglés y español en https://recuperacion.pr.gov/en/resources/policies/general-policies/ y https://recuperacion.pr.gov/en/resources/policies/general-policies/.

La Ley Núm. 141-2019, Ley de Transparencia y Procedimiento Expedito para el Acceso a la Información Pública, 3 LPRA § 9911, según enmendada, establece la política pública del Gobierno de Puerto Rico afirmando que la información y documentación generadas por el gobierno se presumen públicas y de acceso equitativo para todas las personas. Cualquier solicitud de información, o una decisión de denegar su divulgación, debe ser justificada por escrito, citando los fundamentos legales de la negativa dentro de un período de **diez (10) días laborables.**

Sin embargo, el derecho de acceso a la información pública está sujeto a ciertas limitaciones específicas. La Ley de Datos Abiertos del Gobierno de Puerto Rico, Ley Núm. 122-2019, 3 LPRA § 9891, establece el marco para la gestión eficaz de los datos gubernamentales. En virtud de su Sección 4, 3 LPRA § 9894, las entidades gubernamentales pueden invocar reclamos de confidencialidad o privilegio para proteger y retener ciertos datos, siempre que dichos reclamos cumplan con uno o más de los siguientes criterios:

a) La información está protegida por ley;

b) Los datos están cubiertos por privilegios probatorios disponibles para los ciudadanos;
c) La divulgación infringiría los derechos fundamentales de terceros;
d) La información revela la identidad de un informante confidencial; o
e) La información está clasificada como "información oficial" bajo la Regla 514 de las Reglas de Evidencia de Puerto Rico.

En consecuencia, al responder a Solicitudes de Información (**RFI**, por sus siglas en inglés), cualquier PII Sensitiva y Protegida debe ser redactada. En los casos en que apliquen exenciones, como cuando la información solicitada esté legalmente protegida, esté sujeta a privilegios probatorios o su divulgación pueda vulnerar los derechos fundamentales de terceros, la solicitud debe ser denegada. Además, toda negativa de acceso a la información debe ir acompañada de una justificación por escrito que especifique los fundamentos legales de la denegación.

5.2.8 Eliminación de la Información de Identificación Personal

Los expedientes que contienen PII no deben conservarse por más tiempo del requerido. Una vez cumplidos los períodos establecidos para la retención, se deben destruir los expedientes. La disposición adecuada de PII Sensitiva y Protegida conlleva la eliminación **permanente** de los expedientes electrónicos y la trituración de los expedientes impresos.[16]

Vivienda exige que el personal, los contratistas y los subrecipientes de los Programas CDBG-DR/MIT eliminen adecuadamente la PII Sensitiva y Protegida, 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 información de identificación personal de los dispositivos de almacenaje. La disposición 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.

[16] Id.

6 Violación a la Seguridad de PII

La Oficina de Gerencia y Presupuesto (**OMB**, por sus siglas en inglés) define un incidente como "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".[17] A su vez, define una violación como la pérdida de control, compromiso, divulgación no autorizada, adquisición no autorizada o un suceso similar en el que una persona que no es el usuario autorizado tiene acceso o podría tener acceso a información de identificación personal para otros propósitos que no sean los autorizados".[18]

Ejemplos de incidentes que podrían conducir a una violación de la seguridad de PII:

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

6.1 Prevención de violaciones a PII

Para garantizar la protección de la PII y el cumplimiento de esta Política, todos los empleados, contratistas y subrecipientes del Programa CDBG-DR/MIT que tengan acceso a PII o a los sistemas utilizados para recopilar, administrar, transmitir o disponer de la PII deben recibir una capacitación adecuada. Esta capacitación les

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

proporcionará el conocimiento necesario para manejar y proteger la PII de manera efectiva, así como para identificar y responder ante incidentes de seguridad.

Las capacitaciones deberán enfatizar los principios y requisitos establecidos en esta Política y en cualquier documento normativo relacionado, incluyendo, entre otros:

- La importancia de proteger la confidencialidad de la de una persona;
- La identificación de datos que requieren protección;
- La aplicación de medidas de seguridad para resguardar datos y expedientes;
- El almacenamiento adecuado de la información;
- La prevención de divulgaciones de datos indebidas o accidentales; y
- La respuesta ante posibles amenazas a la seguridad.

6.2 Reportar una violación a la seguridad de PII

Todos los empleados de los Programas CDBG-DR/MIT tienen la obligación de reportar de inmediato cualquier incidente sospechoso o confirmado relacionado con PII, vulneración o amenaza potencial, independientemente del medio o formato, a su supervisor. Los empleados deben notificar el incidente sin demora y no deben esperar confirmación de que ha ocurrido una vulneración antes de notificar a su supervisor. El supervisor, a su vez, deberá escalar el incidente a la Oficina de Desarrollo de Políticas, Manejo de Riesgos y Cumplimiento (**PDMRC**, por sus siglas en inglés) de los Programas CDBG-DR/MIT.

Asimismo, los proveedores de servicios de TI, así como cualquier vendedor, suplidor, contratista, subcontratista, consultor, socio o subrecipiente que maneje datos del Programa CDBG-DR/MIT, debe reportar cualquier vulneración de ciberseguridad, incidente o amenaza potencial a la Oficina de PDMRC, así como a la Unidad de Manejo de Subrecipientes.

El informe del incidente, junto con la descripción del mismo, debe incluir información sobre quién, qué, cuándo y cómo ocurrió.

¿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?

El no informar un incidente de manera oportuna puede afectar significativamente la capacidad para contener la vulneración, implementar medidas correctivas y proteger la PII de posibles daños. Se deberá mantener un registro y documentación de la información y las acciones tomadas en relación con el incidente.

6.3 Evaluación de una violación a la seguridad de PII

Al evaluar el tipo y la gravedad de una violación, Vivienda debe considerar tanto la intención como el destinatario de la información comprometida. Al analizar la intención, se evaluará 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 PII divulgada, así como la confiabilidad de dicho destinatario, en caso de ser conocido.[19] Esta evaluación proporcionará un marco de referencia sobre el riesgo relacionado con la posible o confirmada violación a la seguridad de PII.

Los incidentes relacionados con la privacidad pueden clasificarse como de impacto bajo, moderado o alto, según la gravedad del incidente. Los factores que se toman en cuenta para llevar a cabo esta evaluación son: la sensitividad de la PII involucrada, el número de individuos afectados y el daño que podría resultar o que ya ha resultado del incidente.

Impacto Nivel Bajo	Incidente que involucra la divulgación, uso o eliminación no autorizada o indebida de una cantidad limitada de PII

[19] *Id.*

	Sensitiva y Protegida. El impacto es mínimo, afecta a un número reducido de individuos y el daño potencial resultante del incidente es menor.
Impacto Nivel Moderado	Incidente que involucra la divulgación, uso o eliminación no autorizada o indebida de PII Sensitiva y Protegida, lo que podría causar un efecto adverso significativo. Este nivel de incidente puede afectar a un número considerable de individuos y provocar daños sustanciales.
Impacto Nivel Alto	Incidente que involucra la divulgación, uso o eliminación no autorizada o indebida de PII Sensitiva y Protegida, resultando en un efecto adverso grave. Este nivel de impacto incluye la exposición de una cantidad significativa de datos y puede causar daños severos a los individuos afectados.

Aunque existen estos parámetros de clasificación, cada incidente será evaluado caso por caso para garantizar un análisis exhaustivo e integral. Esta evaluación considerará todos los factores relevantes, incluyendo la naturaleza y alcance del incidente, la accesibilidad y sensitividad de los datos comprometidos, el daño potencial o real causado y si se implementaron medidas de mitigación para reducir el riesgo y el impacto de la violación.

Asimismo, como parte de la evaluación, Vivienda determinará si es necesaria la intervención del Área de IT de los Programas CDBG-DR/MIT para evaluar completamente el alcance, la causa y las posibles consecuencias de la violación de seguridad. También se analizará si la gravedad y magnitud del incidente justifican una notificación formal a HUD. Todos los incidentes de alto impacto, debido a su riesgo significativo y el daño potencial, serán reportados a HUD.

6.4 Mitigar el riesgo de una violación a la seguridad de PII

Vivienda y sus proveedores, suplidores, contratistas, subcontratistas, consultores, socios y subrecipientes que manejan datos de los Programas CDBG-DR/MIT deben estar preparados para actuar de inmediato cuando ocurre una violación a la seguridad de PII, para reducir el posible riesgo que podrían enfrentar las personas afectadas. Una vez que se ha realizado una evaluación completa y un análisis de

riesgo, el siguiente paso es aplicar las medidas adecuadas para mitigar el posible daño que la violación, potencial o confirmada, de PII podría causar las personas. Debido a que cada incidente de violación de PII 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 para abordar la violación de seguridad y minimizar el daño potencial:

- **Contramedidas** deben implementarse de inmediato e incluir acciones como contener el incidente, restaurar los sistemas afectados y notificar a las personas impactadas. La selección de las contramedidas adecuadas debe considerar tanto el objetivo inmediato de minimizar el daño a los individuos afectados como la meta a largo plazo de prevenir incidentes similares en el futuro.[20] Un enfoque integral de mitigación garantiza tanto una respuesta efectiva ante la vulneración como la implementación de medidas proactivas para fortalecer la seguridad de PII en el futuro.
- **Orientación** se debe proporcionar información clara a los individuos afectados sobre cómo pueden obtener más detalles sobre la violación de seguridad, así como las acciones recomendadas para proteger su información.
- **Servicios** como recuperación de identidad, monitoreo de crédito, alertas de fraude o asistencia legal. Sin embargo, dado que estos servicios no siempre están disponibles o pueden no abordar completamente los riesgos específicos de cada incidente, se debe proporcionar a los afectados información clara,

[20] Oficina de Privacidad de HUD, Plan de Respuesta a Notificación de Vulneración de HUD, Rev. 1.0, p. 42, 10 de octubre de 2021, https://www.hud.gov/sites/dfiles/OCHCO/documents/3150.1cioh.pdf.

recursos relevantes y orientación sobre medidas alternativas que pueden tomar para proteger sus datos y mitigar posibles daños.

6.5 Notificación de las violaciones a la seguridad de PII

Las partes afectadas por una violación a la seguridad de PII deben ser notificadas en un plazo de **cuarenta y cinco (45) días**, luego de haber detectado la violación y haber identificado debidamente a las partes afectadas. La notificación debe proporcionar información clara y detallada sobre la vulneración, incluyendo:

- La fecha o período estimado en el que ocurrió el incidente.
- Los tipos de PII involucrados.
- Las contramedidas y/o servicios implementados para mitigar el daño.
- Las acciones que los individuos afectados deben tomar para protegerse aún más.
- Orientación con instrucciones claras sobre cómo los afectados pueden obtener más información sobre la vulneración, incluyendo un punto de contacto designado para consultas adicionales y sus datos de contacto.
- Acciones recomendadas que pueden tomar para fortalecer su protección.

Los contratistas, subcontratistas, consultores o subrecipientes responsables de emitir las notificaciones de las violaciones de seguridad deben certificar a Vivienda que las notificaciones requeridas han sido realizadas conforme a esta Política. Dicha certificación deberá incluir documentación que confirme la fecha, el método y los destinatarios de la notificación, así como un resumen de la información proporcionada. Vivienda se reserva el derecho de solicitar detalles adicionales para asegurar el cumplimiento con los requisitos de notificación y reafirmar su compromiso con la transparencia y la protección de la PII.

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 Núm. 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 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 Núm. 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:

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

[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).

través de las publicaciones o la programación de mayor circulación orientada a ese sector.[23]

6.6 Requisitos para Contratistas, Subrecipientes y otros Socios

Vivienda requiere que todos sus contratistas, subrecipientes, socios y al personal de los Programas CDBG-DR/MIT cumplan o superen los estándares establecidos en esta Política, asegurando su correcta adopción y administración. En consecuencia, los contratos y acuerdos de subrecipiente de los Programas CDBG-DR/MIT incluyen disposiciones para proteger la información confidencial y sensitiva, prohibiendo su uso, venta, comercialización o divulgación a terceros sin el consentimiento por escrito de Vivienda.

Los contratistas, subrecipientes y socios deben asegurarse de que sus políticas de PII incorporen capacitación integral, prácticas de gestión eficaces y protocolos sólidos de respuesta ante violaciones de seguridad. Asimismo, deben contar con sistemas adecuados que permitan rastrear y monitorear el acceso a PII Sensitiva y Protegida, garantizando su seguridad. Además, deberán facilitar inspecciones o investigaciones para verificar el cumplimiento de esta Política.

Estas medidas permiten a Vivienda responder de manera rápida y efectiva ante cualquier violación de seguridad de PII, ya sea potencial o confirmada. Como parte de los protocolos de respuesta ante violaciones de seguridad, los contratistas, subrecipientes y socios deberán colaborar con Vivienda en el intercambio de información relevante para reportar y gestionar con precisión cualquier incidente de seguridad. Durante este intercambio de información, deberán cumplir con las mejores prácticas del sector en materia de seguridad y protección de datos.

El incumplimiento de esta Política puede dar lugar a acciones disciplinarias por parte Vivienda, así como a la imposición de sanciones y/o condiciones adicionales por parte del HUD, conforme a lo establecido en 2 C.F.R. § 200.338.

[23] Art. 4, 10 LPRA § 4053.

7 Mejores Prácticas Recomendadas para el Manejo Seguro de la PII

El personal de Vivienda, sus subrecipientes, contratistas, subcontratistas, y otros socios junto con su equipo de trabajo, deben proteger la información confiada por los solicitantes del Programa. En la gestión y el manejo de PII, se deben implementar diversas estrategias y actividades. 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;
- Recopilar solo la PII necesaria para los fines para los que se recopila;
- Mantener registros precisos sobre dónde se almacena, usa y mantiene la PII en expedientes impresos y electrónicos;
- Auditar periódicamente todas las tenencias de PII Sensitiva para asegurarse de que dicha información pueda localizarse fácilmente;[24]
- Seguir métodos adecuados para la eliminación de documentos que contienen PII; y
- Informar inmediatamente los actos o incidentes sospechados o confirmados de violaciones a la privacidad.

7.2 Identificación 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.
- No deben ser fáciles de adivinar.
- Las contraseñas deben cambiarse con regularidad, según lo determine la Política de Seguridad Informática.

[24] Véase https://www.hud.gov/sites/documents/OHC_PII081214.PDF

- 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 Impresos y Electrónicos

- Los inventarios de PII se mantendrán con listas de identificación de (1) registros impresos; (2) registros electrónicos; (3) registros nuevos, que contengan PII.[25]
- Se debe desarrollar un procedimiento, como compartir recursos de red o utilizar medios removibles, para monitorear y rastrear el movimiento de la PII cuando se copia a otra ubicación autorizada o no autorizada.[26]
- Los expedientes no deberán ser removidos de la oficina sin consentimiento previo, incluso en circunstancias de trabajo remoto.[27]
- El supervisor del empleado/contratista debe otorgar el consentimiento, por escrito, para remover un expediente de la oficina.
- Los archivos que contienen PII Sensitiva, documentos y medios de eliminación, deben estar claramente identificados (ejemplo: Solo Para Uso Oficial, Confidencial).
- Los expedientes impresos se deben mantener en gabinetes de archivo.
- La PII Sensitiva solo se almacenará en estaciones de trabajo ubicadas en áreas que tienen acceso físico restringido.
- 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.
- La protección de archivos electrónicos puede incluir criptografía, implementar autenticación mejorada y limitar el número de personas con acceso a los archivos.
- 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.

[25] Memorandum, HUD OIG Report: HUD PII Records protection and Management, 2019-OE-0002a, 25 de junio de 2020.
[26] *Id.*
[27] *Id.*

- Los expedientes inactivos deberán estar sujetos a la política correspondiente sobre retención de expedientes.
- Todo documento duplicado que contenga información confidencial o sensitiva 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.
- 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 PII.
- 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 PII 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 PII 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.

FIN DE LA POLÍTICA.