OMBUDSMAN

1 9 7 7

Gobierno de Puerto Rico

REGLAMENTO NÚM. 22

REGLAMENTO GENERAL DE LA PROCURADURÍA ESPECIALIZADA DE SISTEMAS DE SEGURIDAD DE BANCOS DE INFORMACIÓN DEL GOBIERNO (PESSBIG)

HON. IRIS MIRIAM RUIZ
PROCURADORA DEL CIUDADANO

OMBUDSMAN
1977
Gobierno de Puerto Rico

OFICINA DEL PROCURADOR DEL CIUDADANO

Hon. Iris Miriam Ruiz Class
Procuradora

REGLAMENTO NÚM. 22

REGLAMENTO GENERAL DE LA PROCURADURÍA ESPECIALIZADA DE SISTEMAS DE SEGURIDAD DE BANCOS DE INFORMACIÓN DEL GOBIERNO (PESSBIG)

Revisado al 27 de abril de 2011

TABLA DE CONTENIDO

Minillas Station PO Box 41088 San Juan, Puerto Rico 00940-1088
Tel. (787) 724-7373 • Fax (787) 724-7386
irismiriam.ruiz@opc.gobierno.pr

Página

ARTÍCULO III
Obligaciones y Responsabilidades de las Agencias

ARTÍCULO IV
Procedimiento de Notificación a la PESSBIG

ARTÍCULO V
Procedimiento de Notificación a las Personas Afectadas

ARTÍCULO VI
Facultades, Obligaciones y Responsabilidades de la PESSBIG

ARTÍCULO VII
Disposiciones Finales

Minillas Station PO Box 41088 San Juan, Puerto Rico 00940-1088
Tel. (787) 724-7373 • Fax (787) 724-7386
irismiriam.ruiz@opc.gobierno.pr

PUERTO RICO VERDE

OMBUDSMAN
1977
Gobierno de Puerto Rico

Hon. Iris Miriam Ruiz Class
Procuradora

OFICINA DEL PROCURADOR DEL CIUDADANO

REGLAMENTO NÚM. 22

REGLAMENTO GENERAL DE LA PROCURADURÍA ESPECIALIZADA DE SISTEMAS DE SEGURIDAD DE BANCOS DE INFORMACIÓN DEL GOBIERNO (PESSBIG)

Revisado al 27 de abril de 2011

ARTÍCULO I

Disposiciones Generales

Sección 1.1 – Título Breve

Este Reglamento se conocerá y citará como "Reglamento General de la Procuraduría Especializada de Sistemas de Seguridad de Bancos de Información del Gobierno (PESSBIG)".

Sección 1.2 – Base Legal

Este Reglamento se adopta en virtud de lo dispuesto en la Ley Núm. 134 del 30 de junio de 1977, según enmendada, conocida como "Ley del Procurador del Ciudadano (Ombudsman)" y la Ley Núm. 111 de 7 de septiembre de 2005, según enmendada, conocida como "Ley de Información al Ciudadano sobre Seguridad de Bancos de Información".

Sección 1.3 – Propósito

Este Reglamento tiene el propósito de proteger a los ciudadanos víctimas de la usurpación de identidad. Asimismo, persigue proteger el buen nombre y el crédito de los ciudadanos, tanto como salvaguardar la integridad de la información personal de éstos. Además, pretende establecer los derechos y responsabilidades de toda agencia que maneje bancos de datos, que incluyan información personal de los ciudadanos o residentes en Puerto Rico. Igualmente, especifica las responsabilidades y obligaciones de toda agencia que provea acceso a

Minillas Station PO Box 41088 San Juan, Puerto Rico 00940-1088
Tel. (787) 724-7373 • Fax (787) 724-7386
irismiriam.ruiz@opc.gobierno.pr

tales bancos de información. Por otra parte, define términos y aclara las facultades de la Procuraduría Especializada de Sistemas de Seguridad de Bancos de Información del Gobierno (PESSBIG).

Sección 1.4 – Aplicación

Las disposiciones de este Reglamento aplican a todas las agencias gubernamentales o corporaciones públicas que posean, custodien, almacenen o mantengan un banco de información o datos que incluya información personal de ciudadanos o residentes en Puerto Rico.

ARTÍCULO II

Definiciones

Los siguientes términos que se mencionen en este Reglamento, tendrán el significado que se expresa a continuación:

Sección 2.1 – Agencia

Significará cualquier agencia, departamento, junta, comisión, división, negociado, oficina, corporación pública o institución gubernamental de la Rama Ejecutiva del Gobierno de Puerto Rico y cualquier funcionario, empleado o miembro de esta rama que actúe o aparente actuar en el desempeño de sus deberes oficiales con excepción de:

a) la oficina propia del Gobernador,
b) los Registradores de la Propiedad en cuanto a las funciones de calificación,
c) la Universidad de Puerto Rico respecto de sus tareas docentes,
d) la Comisión Estatal de Elecciones sobre las facultades, obligaciones y deberes impuestas bajo la Ley Electoral.

Sección 2.2 – Anuncio Público

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

Sección 2.3 – Archivo de Información Personal

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

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

No se incluye, dentro de la información protegida, la dirección postal o residencial ni información que sea documento público y esté disponible para la ciudadanía en general. Los expedientes podrán ser electrónicos, escritos o audiovisuales, sin que se limiten a estos tipos.

Sección 2.4 – Bancos de Información

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

Sección 2.5 – Ciudadano

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

Sección 2.6 – Clave Criptográfica ("Encripted")

Es una escritura que se utiliza como clave secreta o para controlar una operación.

Sección 2.7 – Oficina

Se refiere a la Oficina del Procurador del Ciudadano (Ombudsman).

Sección 2.8 – Procurador(a)

Se refiere a el (la) Procurador(a) del Ciudadano (Ombudsman).

Sección 2.9 – Procurador(a) Especializado(a) de Sistemas de Seguridad de Bancos de Información del Gobierno (PESSBIG)

Funcionario(a) designado(a) por el (la) Procurador(a), adscrito a su Oficina, encargado(a) de trabajar los casos de violación o irregularidad en los sistemas de seguridad de los bancos de información en una agencia.

Sección 2.10 – Persona

Incluye las personas naturales y jurídicas.

Sección 2.11 – Robo de Identidad

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

Sección 2.12 – Violación de la Seguridad del Sistema

Cualquier situación en que se detecte que se ha permitido el acceso de personas o agencias no autorizadas a los archivos de información personal, de modo que la seguridad, confidencialidad o integridad de la información en el banco de datos quede en entredicho. También incluye, cuando exista acceso por personas o agencias normalmente autorizadas y se conozca o se sospeche que se ha violado la confidencialidad profesional u obtuvieron su autorización bajo falsas representaciones con la intención de hacer uso ilegal de la información. Incluye tanto el acceso a los bancos de información a través del sistema, como el acceso físico a los medios que los contienen y cualquier sustracción o movimiento indebido de los mismos.

ARTÍCULO III

Obligaciones y Responsabilidades de las Agencias

Sección 3.1 – Notificación a los Ciudadanos

Toda agencia propietaria o custodia de un banco de datos que incluya información personal de los ciudadanos o residentes en Puerto Rico, deberá notificar a dichas personas de cualquier violación de la seguridad del sistema cuando los bancos de información cuya seguridad fue violada, contuviera todo o parte de su archivo de información personal y la misma no estuviera protegida con claves criptográficas más allá de una contraseña. La notificación, según descrito en la Sección 5.2, deberá ocurrir dentro de los tres (3) días laborables de haber ocurrido la violación de la seguridad del sistema o desde que se tuvo conocimiento de ello.

Sección 3.2 – Notificación a la PESSBIG

Toda agencia propietaria o custodia de un banco de datos que incluya información personal de los ciudadanos o residentes en Puerto Rico, deberá notificar a la PESSBIG de cualquier violación de la seguridad del sistema que haya permitido el acceso a los archivos por personas no autorizadas. La notificación, según descrita en la Sección 4.1, deberá presentarse inmediatamente de haber ocurrido la violación de la seguridad del sistema o desde que se tuvo conocimiento de ello.

Sección 3.3 – Protección de Información Personal

Toda agencia que posea, almacene, mantenga o guarde información personal sobre un ciudadano o residente de Puerto Rico, deberá desarrollar, implementar, mantener y monitorear un programa de seguridad para proteger los bancos de dicha información. El Programa de Seguridad debe ser razonablemente consistente con los parámetros mínimos establecidos por la industria de programas de dicha índole y contener salvaguardas administrativas técnicas y físicas para garantizar la seguridad y confidencialidad de los archivos de información personal.

Sección 3.4 – Estándares Generales para la Protección de Información Personal

Las agencias deberán aprobar medidas o programas de seguridad que protejan la información personal, conforme con las reglamentaciones existentes según las precedentes secciones de este artículo, tomándose en consideración:

a) ámbito y tipo de servicio que provea la agencia obligada de proteger la información personal;
b) los recursos económicos disponibles con los que cuenta dicha agencia;
c) la cantidad de información almacenada;
d) la cantidad de personas en riesgo; y
e) la necesidad de seguridad y confidencialidad de la información del ciudadano así, como de la información de la agencia y sus empleados.

Sección 3.5 – Estándares Específicos para la Protección de Información Personal

Sin limitar la generalidad de la sección anterior, todo Programa de Seguridad de información establecido por una agencia debe incluir, como mínimo:

a) Designar uno o más empleados para mantener el programa de seguridad.
b) Identificar y evaluar los riesgos internos y externos previsibles, a la seguridad, confidencialidad o integridad de cualquier documento ya sea escrito, electrónico, o de cualquier otra forma, que contenga información personal. Además, evaluar y mejorar la efectividad de las salvaguardas actuales para limitar tales riesgos, incluyendo pero sin limitarse a:
    1. entrenamiento para empleados, incluyendo temporeros y contratistas;

2. cumplimiento de los empleados con las políticas y procedimientos; y
3. medios para detectar y prevenir fallas en el sistema de seguridad.

c) Desarrollar políticas de seguridad para empleados, tomando en cuenta la manera y si a éstos debe permitírsele mantener, acceder y transportar archivos que contengan información personal fuera de las facilidades de la agencia.

d) Imponer medidas disciplinarias por violaciones a las reglas del Programa de Seguridad.

e) Prevenir que empleados cesanteados accedan a los archivos que contengan información personal mediante la terminación inmediata de su acceso físico y electrónico a tales archivos, incluyendo la desactivación de los nombres de usuarios y contraseñas.

f) Tomar todas las medidas razonables para verificar que cualquier proveedor de servicios con acceso a información personal tenga la capacidad de proteger la misma en la manera provista en este Reglamento. Además, deberá asegurarse que tal proveedor de servicio esté aplicando a esa información personal medidas de seguridad por lo menos igual de rigurosas como las que se requiere en este Reglamento. Una vez finalice la prestación del servicio o caduque la vigencia del contrato, remover de inmediato el acceso de éstos al sistema de información.

g) Limitar la cantidad de información personal que sea necesaria para llevar a cabo el propósito legítimo para la cual es reunida; limitar el acceso a esas personas quienes son requeridas para conocer tal información, a fin de lograr tal propósito o cumplir con los requisitos estatales o federales de retención de archivos.

h) Identificar archivos electrónicos, en papel y de cualquier otra índole, sistemas de informática y artículos almacenados, incluyendo computadoras y aparatos portátiles usados para almacenar información personal. Esto no será necesario cuando el Programa de Seguridad de información provea para el manejo de todos los documentos como si todos contuvieran información personal.

i) Establecer restricciones sobre el acceso físico a los archivos que contengan información personal, incluyendo un procedimiento escrito que exponga la forma

en que el acceso físico a esos archivos es restringido y el almacenamiento de tales archivos e información en facilidades cerradas.

j) Monitoreo regular de los usuarios que acceden al sistema de banco de datos para garantizar que el Programa de Seguridad es operado con el propósito de prevenir el acceso o el uso desautorizado de información personal, modernizando las medidas de seguridad según sea necesario.

k) Revisar el alcance de las medidas de seguridad, anualmente, o siempre que haya un cambio sustancial en las prácticas de la industria que puedan comprometer la seguridad o integridad de los archivos que contengan información personal.

l) Documentar acciones responsivas tomadas en conexión con cualquier incidente que envuelva una violación a la seguridad, y una revisión obligatoria sobre los eventos y acciones tomadas luego del incidente para hacer cambios en las medidas de protección de información personal.

ARTÍCULO IV

Procedimiento de Notificación a la PESSBIG

Sección 4.1 – Notificación

La agencia a la cual se violó la seguridad de sistema de información informará a la PESSBIG por escrito dentro de un plazo de veinticuatro (24) horas a partir del momento en que se detecte dicha violación.

Sección 4.2 – Contenido de la Notificación

La notificación de violación de la seguridad del sistema que haga la agencia a la PESSBIG, deberá indicar:

1. la fecha de la violación al sistema de información;
2. el número de ciudadanos potencialmente afectados;
3. si se ha identificado los ciudadanos afectados;
4. si se ha notificado a éstos, cualquier investigación que se encuentre en curso;
5. la naturaleza de la situación;
6. qué medidas está tomando al respecto y
7. un estimado del tiempo requerido para rectificar la situación.

ARTÍCULO V

Procedimiento de Notificación a las Personas Afectadas

Sección 5.1 – Notificación Expedita

La notificación a las personas que habrá de hacer la agencia, según requerida en la Sección 3.1, deberá ser de la manera más rápida posible, tomando en consideración la necesidad de las agencias del orden público de asegurar posibles escenas de delito y pruebas, así como de la aplicación de medidas necesarias para restaurar la seguridad del sistema. En caso del incumplimiento de parte de la agencia, la PESSBIG podrá hacer la debida notificación por cualquier medio disponible.

Sección 5.2 – Contenido de la Notificación

La notificación de violación de la seguridad del sistema deberá indicar, hasta donde lo permita, la siguiente información:

a) una descripción general de lo ocurrido;
b) la naturaleza de la información personal del ciudadano que pudo estar en riesgo en el incidente;
c) lo que la agencia ha hecho para proteger la información personal del ciudadano de futuras violaciones a la seguridad de su información;
d) las diversas acciones que los ciudadanos pueden tomar para protegerse del robo de identidad;
e) cualquier investigación que se encuentre en curso; y
f) el número de ciudadanos potencialmente afectados.

Sección 5.3 – Derecho de las Personas

En caso de que se conozca que se violó la confidencialidad de la información de una persona identificable, tendrá derecho a conocer qué información fue objeto de la violación de confidencialidad.

Sección 5.4 – Opciones de Notificación

Para notificar a las personas, la agencia tendrá las siguientes opciones:

a) Notificación escrita a los afectados por vía personal, postal o electrónica autenticada de acuerdo con la Ley de Firmas Digitales; y

b) Cuando el costo de notificar a todos los potencialmente afectados de acuerdo al inciso anterior sea oneroso por la cantidad de personas afectadas, la dificultad en localizar a todas las personas, o la situación económica de la agencia; o siempre que el costo exceda los cien mil ($100,000) dólares, o el número de personas afectadas exceda de cien mil (100,000), la agencia llevará a cabo su notificación mediante los siguientes dos pasos:

1. despliegue prominente de un anuncio al respecto en el local de la agencia, en la página electrónica de la agencia, si alguna, y dentro de cualquier volante informativo que publique y envíe a través de listas de correo, tanto postales como electrónicas; y
2. comunicación al respecto a los medios de prensa, incluyendo en un periódico de circulación general diaria, que informe de la situación y provea información sobre cómo comunicarse con la agencia para darle mayor seguimiento. Además, cuando la información sea de relevancia para un sector profesional o comercial específico, podrá efectuar este anuncio a través de las publicaciones o la programación de mayor circulación orientada a ese sector. La publicación en el periódico de circulación general diaria nunca será menor a un cuarto de página.

ARTÍCULO VI

Facultades, Obligaciones y Responsabilidades de la PESSBIG

Sección 6.1 – Procedimientos de la Investigación

La PESSBIG investigará, salvo lo dispuesto en la Sección 6.2, las violaciones a los sistemas de seguridad donde se encuentren bancos de información personal. La PESSBIG podrá utilizar los procedimientos establecidos en los Reglamentos 1, 2 y 3 de la Oficina, según facultados por la Ley Núm. 134.

Al realizar cualquier investigación, la PESSBIG podrá hacer las pesquisas y obtener la información que estime necesaria a los fines de la misma. A tales efectos, las agencias deberán dar acceso a los funcionarios y empleados de la PESSBIG, a todos sus archivos y documentos.

A los fines de la investigación, la PESSBIG podrá celebrar aquellas audiencias privadas e inspecciones oculares que estime pertinentes. Así como, tomar juramentos y declaraciones, ordenar la comparecencia y declaración de testigos y requerir la presentación de cualesquiera papeles, libros, documentos y otra evidencia.

Sección 6.2 – Deber de Identificar Medidas de Seguridad tomadas por las Agencias

La PESSBIG podrá realizar revisiones periódicas en las agencias, mediante las cuales identificará las medidas de seguridad tomadas por éstas, para proteger los bancos de información que se encuentren bajo su poder. Deberá corroborar que las medidas a los protocolos de seguridad cumplan con las disposiciones de este Reglamento.

Sección 6.3 – Términos para acoger las recomendaciones de la PESSBIG

Cuando la PESSBIG adquiera conocimiento de agencias que no cuenten con un programa de seguridad para información personal o que el mismo sea deficiente, podrá recomendar a las mismas que desarrollen e implementen un programa de seguridad que cumpla con los requisitos mínimos que establece el presente Reglamento. Establecerá un término, que en ningún caso será mayor de seis (6) meses, dentro del cual la agencia deberá cumplir con sus recomendaciones tomando en consideración los estándares establecidos en la Sección 3.4 del presente Reglamento.

Sección 6.4 – Deber de Notificación a la PESSBIG sobre Cumplimiento con sus Recomendaciones

La agencia notificará a la PESSBIG del cumplimiento de sus recomendaciones dentro del plazo establecido, según dispone la sección anterior del presente Reglamento. Dicha notificación deberá incluir una explicación del programa de seguridad diseñado e implementado y la fecha en que el mismo entrará en vigor.

Sección 6.5 – Informes de la PESSBIG

Luego de la investigación realizada, la PESSBIG redactará un informe donde se incluyan los hallazgos, recomendaciones o conclusiones el cual será enviado a la agencia investigada. La PESSBIG deberá publicar sus informes de investigación y de entender pertinente hará los referidos correspondientes.

ARTÍCULO VII

Disposiciones Finales

Sección 7.1 – Derogación

Se deroga el Reglamento Núm. 22, aprobado el 17 de septiembre de 2009, según enmendada y cualquier disposición incluida en Carta Circular, Orden Administrativa o escrito contrario a lo dispuesto en este Reglamento.

Sección 7.2 – Cláusula de Separabilidad

Si cualquier parte, párrafo o cláusula de este Reglamento fuese declarada nula por un Tribunal con jurisdicción competente, la sentencia dictada a tal efecto sólo afectará aquella parte, párrafo o cláusula cuya nulidad haya sida decretada.

Sección 7.3 – Vigencia

Este Reglamento comenzará a regir treinta (30) días después de su aprobación por el (la) Procurador(a).

En San Juan, Puerto Rico, a 27 de abril de 2011.

HON. IRIS MIRIAM RUIZ CLASS
Procuradora del Ciudadano

Minillas Station PO Box 41088 San Juan, Puerto Rico 00940-1088
Tel. (787) 724-7373 • Fax (787) 724-7386
irismiriam.ruiz@opc.gobierno.pr