GUIA PARA LA GESTIÓN, DOCUMENTACIÓN Y COMUNICACIÓN DE VULNERACIONES DE SEGURIDAD EN DATOS PERSONALES

Índice

1. Introducción
2. Definiciones
3. La seguridad de los datos y la protección de datos personales

   3.1 Principio de Seguridad de los Datos

   3.2 Algunas recomendaciones en materia de medidas de seguridad

4. Gestión y comunicación de una vulneración de seguridad de datos personales

   4.1 Sujetos intervinientes

   4.2 Plazos

   4.3 Contenido de las comunicaciones

5. Gestiones posteriores a la comunicación de la vulneración de seguridad

Anexo: Datos necesarios para la comunicación de vulneración de seguridad de datos personales

1. Introducción

La Unidad Reguladora y de Control de Datos Personales (URCDP) ha publicado diversas guías que refieren a temas vinculados con el derecho de protección de datos personales, derecho humano que tiende a proteger a los titulares de los datos, ya sean personas físicas o jurídicas en lo que se estime pertinente, cuyos datos se encuentren recolectados, tratados y almacenados en bases de datos pertenecientes a responsables tanto en el ámbito público como en el privado.

En este marco, es necesario contar con una guía que permita orientar sobre cómo documentar y notificar las vulneraciones de seguridad, considerando especialmente al principio de seguridad de los datos, el principio de responsabilidad proactiva, y las nuevas obligaciones impuestas en la materia (artículos 10 y 12 de la Ley N° 18.331, de 11 de agosto de 2008, y artículos 38 y 39 de la Ley N° 19.670, de 15 de octubre de 2018).

Es importante recordar que en la interpretación y aplicación de la Ley no basta con considerar únicamente uno o dos principios aislados, sino que debe ser vista de forma integral; integralidad que debe aplicarse en la solución de potenciales vulnerabilidades y en medidas correctivas ante efectivas vulneraciones.

Esta guía está orientada a los responsables y encargados de bases de datos o de tratamiento de datos personales según lo establecido en el artículo 4° lit. D de la Ley N° 18.331. Esto es, a quienes traten información de cualquier tipo referida a personas físicas o jurídicas determinadas o determinables y que pueden verse afectadas por brechas o incidentes de seguridad.

Si esto sucede, los responsables y los encargados en su caso deberán gestionar dichas brechas o incidentes, documentar las operaciones realizadas y notificar a la URCDP, siguiendo todos los procedimientos necesarios y adecuados, de forma sencilla y dinámica.

En esta guía no sólo se brinda apoyo a responsables y encargados de las bases de datos o de tratamiento, sino también a todas las personas que, de una forma u otra, están trabajando con datos personales (profesionales actuando por cuenta de sus clientes, técnicos, empleados, cobradores, recolectores, etc.).

Se especificarán cuáles son las medidas que se deben observar en el momento de la vulneración, los plazos legales a cumplir, la gestión y comunicación tanto

al principio como al final, y las recomendaciones que la URCDP pretende llevar a los sujetos obligados.

2. Definiciones

Para lograr un criterio único de interpretación de los conceptos que se manejan a lo largo de esta guía, se incluyen algunas definiciones:

Incidente de seguridad: acceso, intento de acceso, uso, divulgación, modificación o destrucción no autorizada de información; un impedimento en la operación normal de las redes, sistemas o recursos informáticos; o una violación a la política de seguridad de la información del organismo (Acceder a incidente de seguridad-Certuy).

Medidas de seguridad: medidas técnicas y organizativas necesarias para conservar la integridad, confidencialidad y disponibilidad de la información, de forma de garantizar la seguridad de los datos personales[1].

Vulnerabilidad de seguridad: debilidad o fallo en un sistema de información que pone en riesgo la seguridad de la información, pudiendo permitir que un atacante pueda comprometer la integridad, disponibilidad o confidencialidad de la misma, por lo que es necesario encontrarlas y eliminarlas lo antes posible. Estos «agujeros» pueden tener distintos orígenes, por ejemplo: fallos de diseño, errores de configuración o carencias de procedimientos (Acceder a vulnerabilidad de seguridad en Incibe).

Vulneración de seguridad: incidente de seguridad que ocasione, entre otras, la divulgación, destrucción, pérdida o alteración accidental o ilícita de datos personales, o la comunicación o acceso no autorizados a dichos datos[2].

En esta guía se tomará la definición incluida en el decreto N° 64/020, de 17 de febrero de 2020 (vulneraciones de seguridad), por ser la vigente a nivel normativo para nuestra materia.

[1] Concepto que resulta del artículo 3° del decreto N° 64/020, de 17 de febrero de 2020.
[2] El artículo 3° del decreto N° 64/020, de 17 de febrero de 2020, hace referencia a la existencia de la existencia de incidentes con el contenido mencionado, y posteriormente en el artículo 4° refiere a la comunicación de vulneraciones de seguridad, por lo que se desprende que la descripción referida en el artículo anterior se compadece con el último de los conceptos mencionados.

3. La seguridad de los datos y la protección de datos personales

3.1 Principio de Seguridad de los Datos

Uruguay cuenta desde el año 2008 con la Ley N° 18.331, de 11 de agosto, de Protección de Datos Personales y Acción de Habeas Data.

En ella se regulan diversos principios en sus artículos 5° al 12°, a los que se deben ceñir los responsables y encargados de tratamiento de las bases de datos ya sean públicos o privados. Estos servirán también para interpretar y resolver controversias que puedan aparecer cuando sean aplicados.

Dentro de estos principios se encuentra el que es el objeto central de esta guía: el de seguridad de los datos, regulado en el artículo 10 de la Ley N° 18.331[3]. Este principio refiere a las medidas de seguridad que deben ser adoptadas, pero además establece obligaciones vinculadas a la forma de almacenar los datos –de forma de permitir el ejercicio del derecho de acceso- y a condiciones técnicas de integridad y seguridad de bases de datos, que, de no existir, prohíben el registro de dichos datos.

La adopción de medidas de seguridad en base a este principio y la comunicación de vulneraciones de seguridad se encuentran reglamentadas además en el decreto N° 414/009, de 31 de agosto de 2009 (artículos 7° y 8°).

El régimen incluido en los artículos de la Ley y los decretos citados fue modificado por el artículo 38 de la Ley N° 19.670, y por los artículos 3° y 4° del decreto N° 64/020.

Con las modificaciones efectuadas por ley y el decreto, el responsable de la base de datos y el encargado de su tratamiento en su caso, tienen la obligación de adoptar las medidas de seguridad necesarias para conservar la integridad,

[3] El artículo 10° indica que: "*El responsable o usuario de la base de datos debe adoptar las medidas que resultaren necesarias para garantizar la seguridad y confidencialidad de los datos personales. Dichas medidas tendrán por objeto evitar su adulteración, pérdida, consulta o tratamiento no autorizado, así como detectar desviaciones de información, intencionales o no, ya sea que los riesgos provengan de la acción humana o del medio técnico utilizado.*
Los datos deberán ser almacenados de modo que permitan el ejercicio del derecho de acceso de su titular.
Queda prohibido registrar datos personales en bases de datos que no reúnan condiciones técnicas de integridad y seguridad."

confidencialidad y disponibilidad de la información, de forma de garantizar la seguridad de los datos personales.

Se evoluciona así desde el concepto de medidas "idóneas" previsto en el decreto 414/009, al de medidas "necesarias", aproximándose al alcance previsto en el artículo 10° de la Ley N° 18.331, lo que significa un mayor énfasis en la adopción de éstas, para evitar vulneraciones de seguridad.

Para que esa garantía sea suficiente y consigne que esa información se encuentra segura, se tendrá en cuenta que, tanto las personas responsables o encargadas de tratamiento deberán seguir estándares nacionales e internacionales en el tema. El propio decreto sugiere la valoración del Marco de Ciberseguridad desarrollado por la Agencia para el Desarrollo del Gobierno de Gestión Electrónica y la Sociedad de la Información y del Conocimiento (Agesic). (Acceder a Marco de Ciberseguridad).

Por lo tanto, las medidas que se utilicen deberán proteger a la información que contiene datos personales de ser la divulgada, destruida, perdida o alterada accidental o ilícitamente, o que se comunique o se dé acceso no autorizado a dichos datos.

Por otra parte, la adopción de medidas de seguridad se encuentra intrínsecamente vinculada al principio de responsabilidad proactiva, siendo la valoración de los riesgos y la adopción de medidas de mitigación parte integral de las evaluaciones de impacto previstas en el artículo 12 de la Ley N° 18.331, en la redacción dada por el artículo 39 de la Ley N° 19.670 y en los artículos 5° a 7° del decreto N° 64/020 (Acceder a Guía de Evaluaciones de Impacto URCDP-AAIP).

En resumen, el principio de seguridad involucra a responsables y encargados de tratamiento de las bases de datos en toda actividad de tratamiento de datos, obligaciones de gestión, documentación, y comunicación, cada vez que se produzca una vulneración o incidente en los que el objeto sea los datos personales tratados.

3.2 Algunas recomendaciones en materia de medidas de seguridad

A continuación, se presentan algunas recomendaciones para las personas responsables y encargadas de tratamiento:

a) Usar los sistemas y software necesarios para tener el nivel de seguridad adecuado, según el tipo de dato tratado.
b) Determinar en forma correcta, eficaz y eficiente quiénes son las personas que tienen los permisos para la gestión de los datos personales que contienen las bases y su acceso.
c) Utilizar contraseñas seguras, difíciles de ser descifradas por terceros.
d) Instalar programas conocidos o que se pueda identificar el origen.
e) Publicar sólo los datos personales necesarios.
f) Realizar copias de seguridad de los datos personales que se posee, las que deberán almacenarse al menos con los mismos criterios de seguridad que la base original.
g) Usar servicios de nube de proveedores conocidos y con criterios seguros para los datos personales.

4. Gestión y comunicación de una vulneración de seguridad de datos personales

Ya se mencionó el concepto de dato personal, referente a toda información de cualquier tipo referida a personas físicas o jurídicas determinadas o determinables. Alcanza por ende a todo dato personal que, a pesar de no identificar directamente a la persona, la hace identificable en forma indirecta (llegamos a ella por él, pero efectuando más de un paso).

Entonces, la vulneración de seguridad sobre datos personales puede referir a datos que son identificatorios directamente de quien es su titular, pero también a otros datos que, sin que se le identifique directamente, vuelven al titular identificable. Esto requiere un régimen de seguridad mucho más sólido.

En consecuencia, la gestión y comunicación de las vulneraciones deben contener las mayores garantías para quien es titular de los datos vulnerados, así

como una buena integralidad, lo que se acentúa si esos datos personales son sensibles o especialmente protegidos según lo establecido en la normativa referida al tema.

4.1 Partes intervinientes

Se puede dividir la gestión de datos en base a las diversas partes que intervienen en ella, ya sea porque se ven involucradas o perjudicadas. Estos son:

1) Responsables y encargados de tratamiento: deben asegurarse que desde la recolección hasta la eliminación de los datos (incluyendo etapas como el bloqueo), se consideren las mayores garantías en materia de seguridad para el cumplimiento de los principios establecidos en la norma.

Se debe tener presente que la Ley menciona que los encargados de una base o de tratamiento deben cumplir con las mismas obligaciones de quienes son responsables de la base de datos, referentes al principio de seguridad, ya que los pone en un plano de igualdad (artículo 38 Ley N° 19670).

No obstante, en lo que hace estrictamente a las comunicaciones de vulneraciones de seguridad, existen desde la reglamentación algunas diferencias que se verán más adelante.

2) Unidad Reguladora y de Control de Datos Personales (URCDP): recibe la información del responsable (y eventualmente del encargado de tratamiento) y comienza con su trámite interno basado en el decreto 500/991, de 27 de setiembre de 1991. El artículo 38 de la Ley N° 19.670 prevé la actuación del Centro Nacional de Respuesta a Incidentes de Seguridad Informática del Uruguay (CERTuy – Acceder al sitio), con quien la URCDP evaluará el contenido de la comunicación y las medidas adoptadas, y se pondrá de acuerdo con el procedimiento a seguir, lo que se comunicará al responsable o al encargado en su caso.

3) Titular del dato personal: definido este en el artículo 4° lit. L de la Ley N° 18.331, como la persona cuyos datos sean objeto de un tratamiento incluido

dentro de su ámbito de acción. El régimen de la Ley se aplica a la persona, pero también a la persona jurídica en lo que sea pertinente (artículo 2° de la Ley).

4) Delegado de protección de datos personales: este se encuentra presente en todos los casos que la norma de protección de datos personales, sus modificativas y decretos lo establecen como obligatorios: entidades públicas, estatales o no estatales, privadas total o parcialmente de propiedad estatal, entidades privadas que traten datos sensibles como negocio principal y las que realicen el tratamiento de grandes volúmenes de datos, entendiéndose como tal cualquier actividad en la que se realice tratamiento de datos personales de más de 35.000 datos personas[4].

La persona designada como delegada, tendrá un papel importante y relevante en todos los aspectos del tratamiento de los datos, desde colaborar en la determinación de las medidas de seguridad a adoptar, hasta la redacción de los informes y las comunicaciones tanto a la URCDP como a los titulares de los datos en su caso.

4.2 Plazos

Luego de identificar las partes intervinientes, corresponde considerar los plazos que la normatividad establece para realizar la gestión y comunicación de las vulneraciones.

Ante la constatación de una vulneración de seguridad, tanto el responsable como el encargado en su caso, deben iniciar los procedimientos necesarios para minimizar el impacto de los incidentes dentro de las primeras 24 horas (artículo 3° del decreto N° 64/020).

No obstante, en lo que hace estrictamente a las comunicaciones de vulneraciones de seguridad, existen desde la reglamentación algunas diferencias.

En el caso de quienes son responsables, al conocer la ocurrencia de una vulneración de seguridad debe informar dentro del plazo de 72 horas, dando los mayores detalles posibles del hecho y de las medidas que adoptó hasta el

[4] Ley N° 19.670, art. 40 y Decreto Reglamentario N° 64/020, art. 10.

momento de la comunicación, a la URCDP. Además, si esta vulneración ocasionó una afectación significativa de los derechos de los titulares de los datos, deberá comunicársela a éstos en un lenguaje claro y sencillo (artículo 4° del decreto N° 64/020).

En el caso de los encargados de tratamiento, deben hacer la comunicación directamente a los responsables, quienes deberán proceder en la forma indicada anteriormente. A pesar de ello, puede resultar pertinente y necesario que en determinadas circunstancias los encargados de tratamiento comuniquen directamente a la URCDP la ocurrencia de la vulneración de seguridad, sobre todo en los casos de encargados que tratan datos por cuenta de múltiples responsables (agencias de cobranzas, de correspondencia, entre otras).

Corresponde señalar que, una vez solucionada la vulneración, la persona responsable del tratamiento deberá elaborar un informe pormenorizado de la vulneración de seguridad y las medidas adoptadas y comunicarlo a la URCDP, para el que no se establece plazo. No obstante, éste deberá ser remitido a la brevedad, a efectos de evitar eventuales intimaciones que pueda realizar la Unidad conforme el artículo 34 literal D de la Ley N° 18.331.

4.3 Contenido de las comunicaciones

En este punto deberán tener presente a quiénes se va a comunicar los datos, si será al titular del dato o a la URCDP. En cualquiera de los casos deberá existir un procedimiento previo ya definido por el responsable o el encargado.

Comunicaciones a titulares

El decreto solo exige en el caso de las comunicaciones a los titulares que éstas se realicen en un lenguaje claro y sencillo, para que estos comprendan lo sucedido. La información debe ser lo suficientemente completa para que los titulares de los datos tengan conocimiento de las causas y consecuencias de la vulneración, y de las medidas adoptadas para su subsanación.

No se establecen mecanismos formales para la comunicación, pero sí corresponde que ella sea fehaciente, en tanto debe efectivamente llegar a

quienes son titulares. Pueden pensarse comunicaciones a direcciones físicas, a direcciones electrónicas, o porque no, avisos en el sitio web del responsable o encargado en su caso.

Es fundamental que el responsable o encargado valore la afectación que la vulneración pueda haber producido en los titulares de los datos, máxime cuando se determine la no comunicación a estos, ya que la URCDP requerirá que ello le sea informado, en el marco del cumplimiento de sus cometidos.

Comunicaciones a la URCDP

Las comunicaciones se realizan en base a los dos informes preindicados:

a) El primero se realizará cuando se conoció el incidente y en él se deberán asentar entre otros los siguientes datos:
    a. fecha cierta o estimada de la ocurrencia de la vulneración,
    b. naturaleza,
    c. datos personales afectados,
    d. posibles impactos generados.
b) El segundo informe deberá indicar todos los pormenores de lo sucedido y de las medidas que se adoptaron y realizaron para que esta vulneración haya sido mitigada y no ocurra nuevamente.

Se adjunta a modo de ejemplo y como anexo a esta guía, un ejemplo de los datos necesarios en la comunicación de la vulneración a la URCDP.

5. Gestiones posteriores a la comunicación de la vulneración de seguridad

Como se indicó, la comunicación de las vulneraciones de seguridad no agota las tareas que deben realizar responsables y encargados, que deberán realizar todos los procedimientos necesarios para subsanar sus efectos, y adoptar las medidas para evitar futuras vulneraciones.

La URCDP, por su parte, podrá plantear la necesidad de adoptar nuevas medidas, solicitar correcciones a las existentes (asesorada por el CERTuy), y

requerir ampliaciones de lo informado, además de efectuar en su caso, las actuaciones de fiscalización que estime pertinentes.

La comunicación de la vulneración activa en la Unidad los procesos administrativos correspondientes que se deberán formalizar bajo un expediente que será comunicado oportunamente a los responsables o encargados, y que tendrá como prioridad recolectar la mayor cantidad de información necesaria para determinar la gravedad de la vulneración, la afectación a las personas y los procesos adoptados en forma previa y posterior a ésta.

Los informes elaborados por la URCDP, y en su caso por el CERTuy, serán notificados en forma a los responsables y encargados, cuando corresponda.

Anexo

Datos necesarios para la comunicación de vulneración de seguridad de datos personales

Los sujetos obligados a realizar las comunicaciones deberán completar los siguientes datos:

A. **Datos identificatorios de la persona o entidad que realiza la comunicación:**
   Nombre de la entidad/Nombres y apellidos
   Documento de identificación
   Calidad
   Dirección
   Teléfono
   Correo electrónico

B. **Datos identificatorios del responsable de la base de datos y del delegado de protección de datos personales en su caso:**
   Nombre de la entidad/Nombres y apellidos
   Documento de identificación
   Dirección
   Teléfono
   Correo electrónico
   Nombre del delegado de protección de datos personales
   Correo electrónico del delegado de protección de datos personales

C. **Datos identificatorios del encargado de tratamiento de datos personales (eventual):**
   Nombre de la entidad/Nombres y apellidos
   Documento de identificación
   Dirección
   Teléfono
   Correo electrónico

D. **Datos identificatorios de la base de datos personales:**

Nombre de la base de datos

Ubicación de la base de datos

Número de inscripción de la base de datos en la URCDP (de corresponder)

Cantidad de personas que integran la base de datos

Tipos de datos personales que integran la base de datos

E. **Información temporal de la vulneración de seguridad**

Fecha de inicio (exacta, estimada, no conocida)

Fecha de detección (exacta, estimada, no conocida)

Circunstancias detalladas de su detección:

Si ya se inició el procedimiento para la resolución de la vulneración y sus razones en caso negativo

Si la vulneración ya está resuelta y su fecha de resolución:

Justificación de por qué se notificó tardíamente a la URCDP (después de las 72 horas - eventual)

F. **Información sobre la vulneración de de seguridad (descripción) :**

Referencia del incidente (ejemplos):

- Acceso o difusión no autorizados
- Modificación no autorizada
- Desaparición o pérdida
- Medio por el que se materializó
- Dispositivo perdido, robado o desechado
- Documentación perdida, robada, guardada en lugar no seguro, desechada
- Correo electrónico abierto o perdido
- Eliminación incorrecta de datos en papel
- Datos personales mostrados a la persona incorrecta

- Datos personales utilizados sin el consentimiento del titular
- Publicación no intencionada
- Error humano
- Revelación de datos personales en forma verbal no autorizada
- Datos personales enviados por error
- *Malware*, *Phishing*, o intrusión de un tercero ajeno
- Eliminación incorrecta de datos
- Datos personales enviados por error
- Otros

G. **Medidas preventivas que se realizaron antes de la vulneración**:

H. **Información acerca de los datos personales afectados**

- Datos básicos
- Datos sensibles
- Datos especialmente protegidos
- Datos de localización del titular
- Otros

I. **Información acerca de los titulares de los datos personales**

- Clientes
- Usuarios
- Suscriptores
- Alumnos
- Pacientes
- Otros
- Cantidad de titulares estimados que sus datos fueron vulnerados

J. **Posibles consecuencias de la vulneración (corresponde realizar un detalle de las consecuencias)**

K. **Medidas realizadas para minimizar el impacto de la vulneración (corresponde realizar un detalle de las medidas)**

L. **Comunicación a los interesados:**

Si se comunicó la vulneración de seguridad a los titulares de los datos vulnerados

Fecha en la que se informó o se tiene previsto informar

Número de personas a las que se informó o se tiene previsto informar

Medios o herramientas para la comunicación a los titulares

Justificación para no informar o motivos por los que no se ha informado a la fecha del informe