Introducción

El Reglamento General de Protección de Datos de la Unión Europea (RGPD) en sus artículos 33 y 34 establece como una obligación de seguridad del responsable del tratamiento, la necesidad de registrar las violaciones o brechas de seguridad y en su caso, notificarlas a la autoridad de control y en su caso, a los interesados titulares de los datos afectados por la violación.

Uno de los principios básicos de la protección de datos, recogido en el artículo 5.1.f) del RGPD, es el principio de seguridad. Dicho artículo establece que los datos personales serán tratados de tal manera que se garantice una seguridad adecuada de los datos personales, incluida la protección contra el tratamiento no autorizado o ilícito y contra su pérdida, destrucción o daño accidental, mediante la aplicación de medidas técnicas u organizativas apropiadas («integridad y confidencialidad»).

En el marco de este principio se encuentra la obligación de gestión de brechas o violaciones (en adelante nombradas indistintamente) de seguridad que tiene la entidad responsable del tratamiento de acuerdo a lo establecido en los artículos 33 y 34 del RGPD.

Una violación o brecha de seguridad en materia de datos personales se define como toda violación de la seguridad que ocasione la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos.

Debe por tanto quedar claro que, una violación es un tipo de incidente de seguridad siempre que afecta a datos personales.

Con base en lo anterior, **Fundación de la Comunidad Valenciana Centro de Investigación Príncipe Felipe** (en adelante **CIPF**) ha elaborado la presente política de obligado cumplimiento para todos los empleados del Centro para garantizar el cumplimiento de la obligación de gestión y notificación de brechas de seguridad.

Aprobación de la política

La presente política ha sido aprobada por CIPF.

Modificación de la política

La presente política puede ser modificada por CIPF.

Objeto de la política

Constituye el objeto del presente documento establecer la política destinada al cumplimiento del principio de «seguridad» recogido en el RGPD y concretamente, para garantizar la gestión y en su caso, notificación de brechas de seguridad.

En virtud de lo anterior, se tendrá en cuenta que:

Una violación o brecha de seguridad es aquel incidente que afecta a datos de carácter personal.

- **Tipos de violación o brecha de seguridad:**

Una brecha de seguridad se puede clasificar en una o varias de las siguientes categorías:

- **De confidencialidad:** Tiene lugar cuando personas que no están autorizadas, o no tienen un propósito legítimo para acceder a la información, acceden a ella.
- **De integridad:** Tiene lugar cuando se altera la información original y la sustitución de datos puede ser perjudicial para el titular de los datos.
- **De disponibilidad:** Tiene lugar cuando no se puede acceder a los datos originales cuando es necesario. Puede ser temporal (los datos son recuperables pero tomará un periodo de tiempo y esto puede ser perjudicial para el titular de los datos), o permanente (los datos no pueden recuperarse).

- **Qué hacer ante una brecha de seguridad:**

Una vez que cualquier empleado conoce de la existencia de una brecha de seguridad lo notificará al/a la Delegado/a de Protección de Datos.

- **En qué plazo se realizará esta notificación:**

De forma inmediata.

- **A través de qué medio:**

Correo electrónico corporativo.

- **Qué incluirá dicha notificación:**

Toda la información que el empleado tenga a su disposición y conozca sobre la brecha y al menos, la siguiente:

a) naturaleza de la violación de la seguridad de los datos personales, inclusive, cuando sea posible, las categorías y el número aproximado de interesados afectados, y las categorías y el número aproximado de registros de datos personales afectados;

b) las posibles consecuencias de la violación de la seguridad de los datos personales;

c) en su caso, las medidas adoptadas o propuestas para poner remedio a la violación de la seguridad de los datos personales, incluyendo, si procede, las medidas adoptadas para mitigar los posibles efectos negativos.

Si no fuera posible facilitar la información simultáneamente, y en la medida en que no lo sea, la información se facilitará de manera gradual sin dilación indebida.

Para la notificación de la información anterior, se utilizará el modelo adjunto a esta política como ANEXO I.

- **Qué tramitación seguirá la brecha:**

Tras la notificación realizada por el empleado al/a la Delegado/a de Protección de Datos], CIPF activará un protocolo para el registro y análisis de la brecha en la que se tratará de identificar y clasificar la incidencia y se pondrán en marcha una serie de medidas de contención y reparación de la brecha, así como, la valoración de su posible notificación a la autoridad de control y/o los afectados titulares de los datos.

Obligaciones del personal

Todo el personal señalado en el apartado anterior tiene la obligación de conocer y cumplir la presente política y normativas, medidas y procedimientos derivados de la misma.

El incumplimiento de la presente política o la normativa, medidas y procedimientos derivados de ésta podrá acarrear el inicio de medidas disciplinarias oportunas y, en su caso, las responsabilidades legales correspondientes.

Consultas

Cualquier consulta o sugerencia en relación con la presente política, podrá ser consultada a CIPF.

Efectividad

La presente normativa entrará en vigor el día de su aprobación y quedará publicada para conocimiento y cumplimiento de todos los empleados en el sitio web del CIPF.

ANEXO I
MODELO DE NOTIFICACIÓN

DOCUMENTO NOTIFICACIÓN	
INFORMACIÓN DE LA PERSONA QUE NOTIFICA LA BRECHA DE SEGURIDAD	
Departamento	
Nombre y apellidos	
Puesto	
Correo electrónico	
Teléfono y extensión	
INFORMACIÓN SOBRE LA BRECHA DE SEGURIDAD	
Naturaleza de la violación	
Categorías de interesados afectados	
Número aproximado de interesados afectados	
Categorías de datos personales afectados	
Número aproximado de registros de datos personales afectados	
Posibles consecuencias de la violación de la seguridad de los datos personales	
Medidas adoptadas para poner remedio a la violación de la seguridad de los datos personales	
Medidas propuestas para mitigar los posibles efectos negativos derivados de la violación de la seguridad de los datos personales	
Otras observaciones e informaciones	