Actividad	Todas las actividades del grupo **aqualia**	**Fecha de aprobación**
Área	España y Región Europa	Julio 2018
Unidad de Gestión	Todas las unidades de gestión ubicadas en la Unión Europea	

TÍTULO	**PROCEDIMIENTO DE NOTIFICACIÓN DE VIOLACIONES DE SEGURIDAD DE DATOS DE CARÁCTER PERSONAL**	**CÓDIGO**	**ITG-SI-01**

Alcance

Este documento define el procedimiento a seguir cuando se detecte que ha habido una violación o brecha de seguridad, tanto en medios automatizados (programas, soportes, y equipos informáticos) como no automatizados (medios físicos como el papel) en los que hayan datos personales.

Modificaciones

Nuevo documento.

Indicador	Frecuencia de medida	Estándar	Tolerancia
N/A			

Registros	Lugar de archivo
Comunicaciones de Brechas	e-privacy

	CARGO	NOMBRE
Elaboración	Coordinadora Adjunta Protección de Datos	Carolina Serrano Gallego
Revisión	Técnico Dpto. Sistemas de Gestión	Noemí Pastor Lazcano
Aprobación	Coordinador Protección de Datos	Miguel Perea-Fernández Pacheco

Actividad	Todas las actividades del grupo **aqualia**	**Fecha de aprobación**
Área	España y Región Europa	Julio 2018
Unidad de Gestión	Todas las unidades de gestión ubicadas en la Unión Europea	

TÍTULO	**PROCEDIMIENTO DE NOTIFICACIÓN DE VIOLACIONES DE SEGURIDAD DE DATOS DE CARÁCTER PERSONAL**	**CÓDIGO**	**ITG-SI-01**

¿QUÉ ES UNA BRECHA DE SEGURIDAD?

El Reglamento General de Protección de Datos define **"violación de la seguridad de los datos personales"**, 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**".

¿EN QUÉ PLAZOS HAY QUE NOTIFICAR LA BRECHA DE SEGURIDAD?

Tan pronto como se tenga conocimiento de que se ha producido una violación de la seguridad de los datos personales se debe, sin dilación indebida y, de ser posible, a más tardar **24 horas** después de que haya tenido constancia de ella, notificar la violación de la seguridad de los datos personales.

Es muy importante que se comunique esta brecha de seguridad en el plazo de 24 horas, puesto que el Departamento de Seguridad de la Información tiene que analizar el suceso y en su caso, notificar antes de 72 horas a la Agencia Española de Protección de Datos y a las personas afectadas, en caso de ser necesario por entrañar un riesgo para los derechos y las libertades de las personas físicas.

¿A QUIÉN NOTIFICAR LA BRECHA DE SEGURIDAD?

En España:

Habrá de notificarse la posible violación o incidente de seguridad por correo electrónico al **Dpto. Gestión de Clientes y Protección de Datos de FCC AQUALIA** (protecciondatos@aqualia.es) con el Asunto "**Notificación de brecha de seguridad**".

Para el **resto de Países** se deberá **elaborar una IT específica** por País en la que se identifique el destinatario de la comunicación y la dirección de correo electrónico, y **se deberá especificar que se debe incluir en copia del correo al Dpto. Gestión de Clientes y Protección de Datos de FCC AQUALIA** (protecciondatos@aqualia.es).

Actividad	Todas las actividades del grupo **aqualia**	Fecha de aprobación
Área	España y Región Europa	Julio 2018
Unidad de Gestión	Todas las unidades de gestión ubicadas en la Unión Europea	

TÍTULO	PROCEDIMIENTO DE NOTIFICACIÓN DE VIOLACIONES DE SEGURIDAD DE DATOS DE CARÁCTER PERSONAL	CÓDIGO	ITG-SI-01

¿CÓMO NOTIFICAR LA BRECHA DE SEGURIDAD?

Cuando se haya detectado una posible violación de seguridad o un indicio de un incidente de seguridad o un proveedor o un tercero nos comuniquen una posible brecha de seguridad, se deberá indicar la siguiente **información** a las direcciones de correo electrónico arriba indicadas:

- **Tipo de amenaza**: código dañino, intrusiones, fraude, etc. Se trata de una breve descripción del incidente en función de la información de la que se disponga.
- **Contexto u origen de la amenaza**: interna o externa.
- **Categoría de seguridad de los sistemas y datos afectados**.
- **El perfil de los usuarios afectados**.
- **Datos personales afectados.**
- **Datos legibles/ilegibles**: Datos protegidos mediante algún sistema de seudonimización (por ejemplo, cifrado o hash)
- **Número y tipología de los sistemas afectados.**
- **Número de interesados afectados.**
- **Impacto y consecuencias del incidente en la organización y en los derechos y libertades de los afectados.**
- **Vector de ataque o método**: ruta o medio por el que se ha materializado el incidente. El concepto de "vector de ataque" suele ser uno de los criterios más aceptados a nivel mundial y está directamente relacionado con la identificación del mismo.
- **Si se han adoptado o propuesto medidas para poner remedio a la violación de seguridad de los datos personales.**

Además, y si es posible, se deberá aportar toda la documentación que evidencie la brecha de seguridad y que ayude a detectar la misma.

Ante cualquier duda, hay que dirigirse a la dirección de correo electrónico protecciondatos@fcc.es.