GUÍA DE GESTIÓN DE BRECHAS DE DATOS PERSONALES

ÍNDICE

1. OBJETO Y ALCANCE

El presente procedimiento interno de la Universidad Pontificia Comillas (en adelante "Comillas") establece las directrices para la gestión de brechas de seguridad de datos personales.

Esta guía da cumplimiento a los requisitos establecidos en el RGPD[1], en concreto a que las organizaciones integren dentro de sus políticas internas un procedimiento de gestión de brechas personales que determine y establezca el proceso a seguir en caso de brecha y que sea en todo caso conforme a la normativa.

Además, este documento constituye una medida organizativa de Comillas a efectos de RGPD, ya que tiene como finalidad principal que, ante un incidente de seguridad de datos personales, Comillas responda de forma rápida, ordenada y eficaz. En consecuencia, se minimizan los posibles efectos tanto para los interesados como para Comillas y otros terceros.

En línea con lo anterior, esta guía es de obligado cumplimiento y, en caso de brecha de seguridad, se deben seguir los pasos y aplicar los criterios aquí establecidos.

2. DEFINICIONES

A continuación, se describen las definiciones y/o conceptos de interés que se pueden encontrar en el documento:

- **AEPD**: Agencia Española de Protección de Datos o Autoridad de Control.
- **Brecha de seguridad de datos personales** vs incidente de seguridad:
  - Incidente de seguridad: suceso inesperado o no deseado con consecuencias en detrimento de la seguridad del sistema de la información.
  - Brecha de seguridad de datos personales: violaciones de seguridad que ocasionen la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizado a dichos datos.

  Es decir, todas las brechas de seguridad son incidentes de seguridad, pero no todos los incidentes de seguridad son necesariamente brechas de seguridad.

  A efectos de este documento los conceptos brecha de seguridad, brecha o violación de seguridad debe ser entendido como "Brecha de seguridad de datos personales".

[1] RGPD: Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos)

- **Delegado de Protección de Datos** (**DPD** o **DPO**): En Comillas ostenta este cargo el Secretario/a General en el momento de publicación de esta guía.

  A efectos de la gestión de brechas debe: informar al Responsable/Encargado de las obligaciones y responsabilidades; y cooperar con la Autoridad de Control, actuando como punto de contacto en caso de brechas personales.

- **Encargado del Tratamiento o Encargado**: Persona física o jurídica que trata datos personales por cuenta del Responsable.

  A efectos de la gestión de brechas, será proveedor o tercero y deberá: informar al Responsable de las brechas de los tratamientos encargados, ayudar al Responsable en la gestión de la brecha y ejecutar las tareas de notificación recogidas en caso de que esté así establecido.

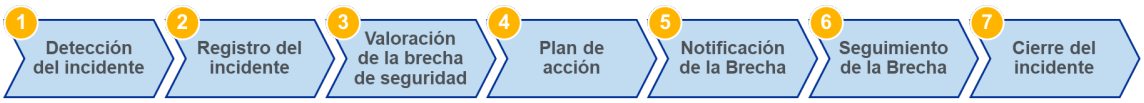
- **Grupo de Trabajo de Protección de Datos o GTPD**: grupo de trabajo que da soporte al DPO para gestionar los asuntos de protección de datos en Comillas. Está compuesto por dos miembros del Servicio de Asesoría Jurídica y al menos un miembro del Servicio de Sistemas y Tecnologías de Información y Comunicaciones (STIC).

- **Responsable del Tratamiento o Responsable**: Persona física o jurídica que determina los fines y medios del tratamiento. Debe aplicar las medidas técnicas y organizativas apropiadas a fin de garantizar y demostrar que los tratamientos de datos se realizan conforme a la normativa.

  A efectos de la gestión de brechas, es Comillas y debe: implantar el proceso de gestión de brechas, evaluar las consecuencias para los derechos y libertades, y notificar la brecha a la autoridad de control y a los interesados, cuando sea necesario.

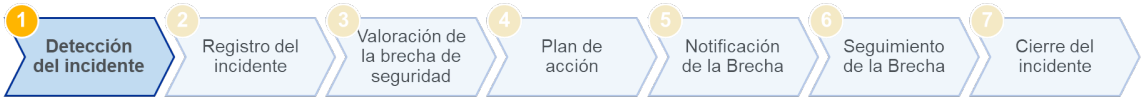
3. PROCEDIMIENTO DE GESTIÓN Y NOTIFICACIÓN

El presente apartado tiene como objetivo definir el proceso para la gestión de las brechas de seguridad en Comillas. Seguidamente se muestra el flujograma de dicho proceso, que consta de 7 fases.



A continuación, se desarrollan cada una de las fases del proceso en los siguientes apartados.

3.1 Detección del incidente

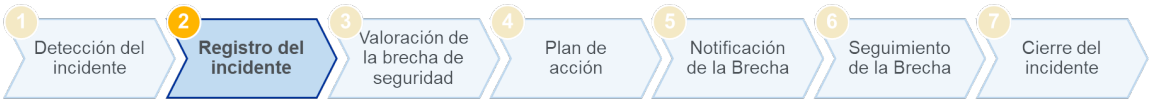


El Personal Docente e Investigador (PDI), el Personal de Administración y Servicios (PAS), o cualquier otro miembro de la comunidad universitaria (fuente interna de comunicación), así como proveedores o terceros (fuente externa de comunicación) deberán notificar a Comillas cualquier brecha de seguridad de datos personales de la que tenga conocimiento[2].

La comunicación de la brecha deberá realizarse preferentemente mediante correo electrónico a la dirección dpo@comillas.edu.

En el caso de que cualquier departamento reciba notificación o tenga conocimiento de una posible brecha de seguridad, deberá igualmente enviar un email sin dilación a la dirección establecida.

3.2 Registro del incidente



El GTPD, será el encargado de recibir las comunicaciones del buzón[3] y evaluar si las situaciones comunicadas constituyen una brecha de seguridad de datos personales.

Una vez comprobado que se trata de una brecha, el GTPD registrará la misma en el "Registro de Brechas de Seguridad[4]" (en adelante el "Registro").

El GTPD podrá requerir la colaboración de las personas que hayan comunicado el incidente con el objetivo de recabar toda la información y evidencias necesarias para completar el Registro.

El Registro tendrá, como mínimo, los siguientes campos:

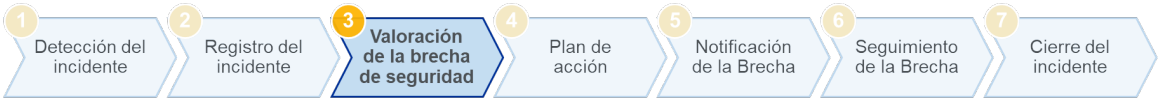
- Tipo de incidente
- Descripción del mismo
- Gravedad
- Estado
- Medidas adoptadas para su resolución
- Comunicación o no a la Autoridad de Control e interesados

[2] A Estos efectos habrá publicada internamente una guía rápida de actuación en caso de que cualquier miembro de la Comunidad Universitaria detecte una brecha de seguridad. Ver Anexo II.

[3] A la dirección dpo@comillas.edu tienen acceso todos los miembros del GTPD y el DPO.

[4] En cumplimiento del art. 33.5 RGPD.

3.3 Valoración de la brecha de seguridad



Con toda la información obtenida se realizará un análisis de la brecha que determinará el tipo y la peligrosidad de la misma. La valoración se realizará conforme a los siguientes criterios:

i) Tipos de brecha de seguridad

Las brechas de seguridad pueden clasificarse en una o varias de las categorías que se indican a continuación en función de la dimensión de seguridad que se hayan visto afectados los datos personales:

Confidencialidad	Cuando partes no autorizadas o sin propósito legítimo para acceder a la información, acceden a ella.
Disponibilidad	Cuando se altera información original y la sustitución de los datos puede ser perjudicial para el individuo.
Integridad	Cuando no se puede acceder a los datos en el momento que se necesita. Puede ser temporal o permanente.

En el Anexo I se puede encontrar una relación de ejemplos de brechas de seguridad en función de su clasificación, así como una descripción más detallada de cada concepto.

ii) Criterios de valoración de brechas de seguridad

Una vez determinado el tipo de brecha, para gestionarla correctamente, se debe evaluar su riesgo en función de los siguientes factores:

- Naturaleza, carácter sensible o no y volumen de los datos personales.
- Facilidad de identificación a las personas.
- Gravedad de las consecuencias para los derechos y libertades de los individuos.
- Características particulares del responsable del tratamiento.
- Impacto de la brecha en la organización, desde los puntos de vista de prestación de servicios, protección de la información, cumplimiento normativo e imagen pública.
- Otras consideraciones generales

iii) Determinación de peligrosidad y magnitud del impacto

En función de la valoración de los criterios anteriores, se realizará un análisis para determinar:

1. La **peligrosidad de la brecha**, en función de las consecuencias para los interesados:

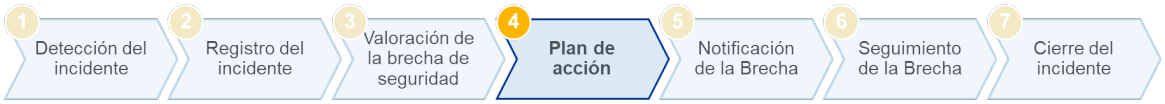
Baja	Los afectados pueden encontrar algunos inconvenientes muy limitados y reversibles, que superarán sin problema.
Media	Los afectados encontrarán inconvenientes importantes, produciendo un daño limitado, que podrán superar a pesar de algunas dificultades.
Alta	Los afectados se enfrentarán a consecuencias significativas, que deberían poder superar, aunque con serias dificultades. Suelen afectar a derechos fundamentales, pero pueden revertirse.
Muy Alta	Los afectados se enfrentan a consecuencias muy significativas o irreversibles, que no se pueden superar. Daña derechos y libertades públicas de forma irreparable.

2. **La magnitud del impacto**:

Posteriormente se deberá determinar si existe la posibilidad de que las consecuencias se materialicen, si aún no se ha materializado el daño, y determinar su probabilidad:

Improbable	Se puede garantizar que el daño no se materializará.
Baja	Cierta probabilidad de materialización del daño.
Alta	Probabilidad razonable de que se materialice el daño.
Muy Alta	Altamente probable de que el daño se materialice.

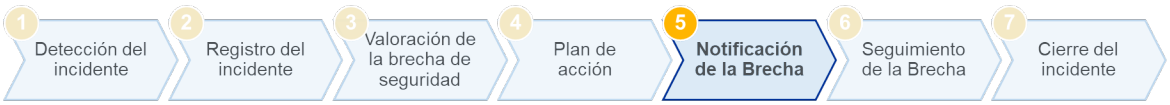
3.4 Plan de acción



Como resultado de la evaluación de la brecha de seguridad el GTPD, con la aprobación del DPO, establecerá el plan de acción para la contención del incidente. El objetivo principal del plan de acción establecer las medidas de seguridad necesarias para mitigar, en la medida de lo posible, el impacto de la brecha.

Las medidas de seguridad acordadas se incorporarán en el Registro.

3.5 Notificación de la brecha



Una vez valoradas las características de la brecha, el GTPD determinará si la misma es susceptible de comunicación a la AEPD, a los afectados y/o a otros destinatarios.

i) Comunicación a la AEPD

El criterio general es que deben ser comunicadas a la AEPD todas las brechas de seguridad de datos personales[5].

Además, la normativa establece un plazo máximo de 72 horas para realizar la comunicación a contar desde que se tenga constancia de que se ha producido una brecha de seguridad de datos personales. A estos efectos, se ha de considerar que "se tiene constancia" desde que hay certeza de que la brecha se ha producido y se tienen conocimientos suficientes de su naturaleza y alcance.

i. Procedimiento de comunicación

Una vez se ha valorado en incidente y se ha determinado que es necesario notificar a la AEPD, se inicia el procedimiento de comunicación.

- En primer lugar, el miembro del GTPD del STIC accederá al **formulario proporcionado por la AEPD** a tal efecto y procederá a realizar la correspondiente comunicación dentro de las **72 horas** posteriores al conocimiento de la brecha. Esta comunicación se realiza mediante el certificado electrónico al que tiene acceso el personal del STIC.
- Una vez confirmado que la presentación se ha hecho correctamente, se pondrá a disposición del GTPD el justificante de presentación, junto con cualquier otra comunicación o documento que se genere.
- En caso de que sea necesario complementar la notificación con más información o documentación se adjuntará a la comunicación original en cuanto se disponga de ella.
- Todas las comunicaciones que se reciban con respecto a la comunicación de la brecha se pondrán en conocimiento del GTPD y se guardarán para llevar un registro de las mismas y poder planificar las siguientes actuaciones, en su caso.

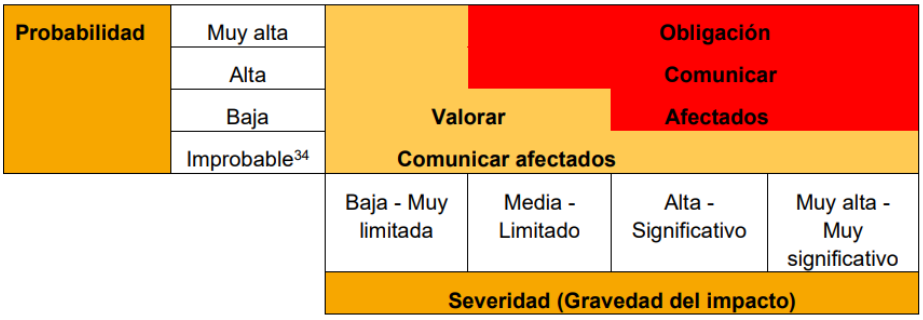
ii) Comunicación a los afectados

Se debe comunicar la existencia de una brecha de seguridad a los afectados, sin dilación indebida, cuando la misma pueda entrañar un alto riesgo para los derechos y libertades de las personas físicas.

Los criterios que valorará el GTPD, con aprobación del DPO, para decidir si se debe realizar esta notificación son:

- Analizar si hay obligaciones contractuales o legales.
- Valorar si el afectado podría evitar o mitigar daños posteriores.
- Los riesgos que entraña la brecha, en función de la valoración previa (apartado 3.2.iii):

[5] Ver definición de violación de datos personales según RGPD, art.4.12 "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



Fuente: AEPD Guía para la notificación de brechas de datos personales

i. Procedimiento de comunicación

Una vez se ha valorado en incidente y se ha determinado que es necesario notificar a los interesados, se inicia el procedimiento de comunicación.

- En primer lugar, el GTPD determinará el **medio a través del cual se realizará la comunicación**.
    - La primera opción será la comunicación directa. La medida más adecuada será el envío de email con confirmación de lectura. Si no fuera posible, se valorarán otros canales como puede ser el envío de SMS, correo postal o llamada de teléfono.
    - Si la comunicación directa no es posible, o sus costes son excesivos, se hará de forma indirecta. Para ello, se publicará la información en la página web, redes sociales o cualquier otro medio de comunicación pública del que disponga Comillas en ese momento.

- Posteriormente el GTPD **acordará el contenido de la comunicación**, que como mínimo incluirá:
    - Los datos de contacto del DPO. En función, del caso concreto el GTPD valorará si se remite la comunicación desde dpo@comillas.edu o prodatos@comillas.edu
    - Una descripción general del incidente y cuándo se ha producido, incluyendo la tipología de datos afectados.
    - Las posibles consecuencias de la brecha de seguridad.
    - Las medidas que han implantado para mitigar los daños.

- Por último, el GTPD **remitirá directamente la comunicación** o colaborará con el servicio correspondiente de Comillas para que se envíe la comunicación.

iii) Excepciones a la notificación

Existen excepciones a las reglas generales de comunicación. No será necesario comunicar a la AEPD o a los interesados la existencia de una brecha de seguridad cuando Comillas pueda demostrar fehacientemente que la brecha no entraña riesgo para los derechos y libertades de las personas físicas. El parámetro determinante para notificar una brecha de datos personales es el **nivel de riesgo para los derechos y libertades de las personas físicas afectadas por la brecha**.

El GTPD, con aprobación del DPO, determinará si es de aplicación esta excepción, para lo que tendrá en cuenta las siguientes consideraciones, entre otras:

- Se han tomado medidas técnicas y organizativas adecuadas de forma previa al incidente que imposibiliten que la brecha tenga un impacto en los afectados.
- Con posterioridad a la brecha, se han tomado medidas de protección que mitiguen total o parcialmente el posible impacto para los afectados
- Cuando la notificación a los afectados suponga un esfuerzo desproporcionado

Se recomienda consultar el documento "Directrices 1/2021 del EDPB"[6] ya que contiene ejemplos que pueden servir de referencia y valoraciones sobre la pertinencia o no de comunicar ciertas incidencias.

[*Además, para complementar el análisis se puede aplicar el modelo indicado por la AEPD a tal efecto, y recogido en el Anexo II de este documento*]

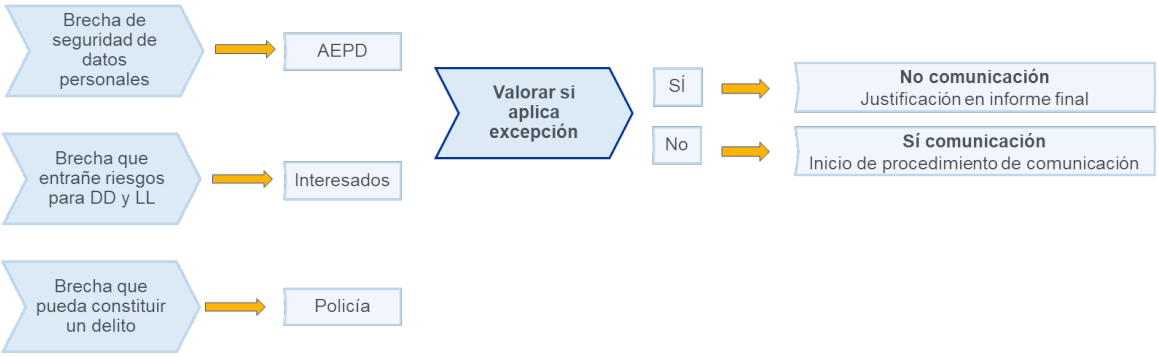
Después de haber realizado este análisis, el GTPD puede determinar que:

- Aplica la excepción y no es necesario realizar ninguna comunicación: Se justificará debidamente esta decisión en el Informe Final.
- No aplica la excepción y es necesario comunicar: Se inician los procedimientos de comunicación explicados anteriormente.

iv) Otras comunicaciones

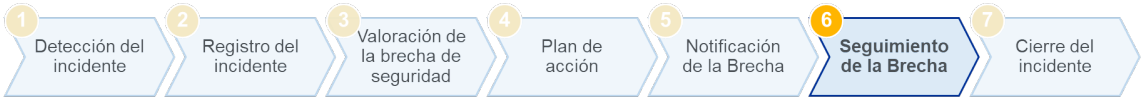
A su vez, el GTPD valorará si es necesario comunicar a otros entes como puede ser la Policía en caso de que haya sospechas de que el incidente pueda ser constitutivo de algún delito.

Procedimiento de notificación de brechas de seguridad:



[6] Acceso al documento: https://edpb.europa.eu/system/files/2022-09/edpb_guidelines_012021_pdbnotification_adopted_es.pdf

3.6 Seguimiento de la brecha

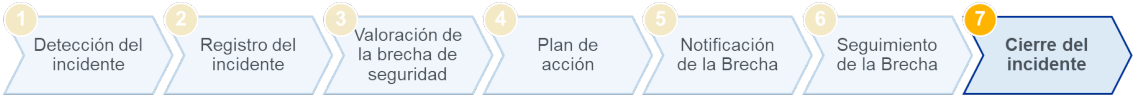


Mientras no se tenga constancia de que la brecha de seguridad está resuelta definitivamente y que ya no hay riesgo para los afectados, no se puede dar por cerrada.

En caso de incidentes que hayan sido comunicados, Comillas estará a disposición de la AEPD para atender cualquier orden de la misma como puede ser un requerimiento de información adicional o una orden de comunicación a los afectados.

En las reuniones de seguimiento entre el DPO y los miembros del GTPD, se repasará el estado de las incidencias abiertas para comprobar si se deben tomar acciones o si se pueden considerar cerradas.

3.7 Cierre del incidente



Una vez se ha mitigado el riesgo para los afectados y se pueda considerar que la brecha está resuelta de manera definitiva, el GTPD elaborará un Informe Final que refleje fielmente lo sucedido, el cual será aprobado posteriormente por el DPO.

El GTPD junto con el DPO valorarán si se debe implementar alguna medida adicional para evitar que se dé la misma situación de nuevo o porque se haya detectado algún error en las medidas de Comillas. Además, se valorará la necesidad de modificar el presente documento para que incorpore información pertinente que no se haya tenido en cuenta.

Anexo I – Ejemplos Ilustrativos de tipos de brechas

Las brechas de seguridad, en función de a qué afecten, se clasifican[7]:

1. Confidencialidad

Una brecha afecta a la confidencialidad cuando los datos personales de un tratamiento han podido ser accedidos por terceros sin permiso, incluyendo cuando los datos son exfiltrados. Esto incluye, por ejemplo, los casos de intrusión en sistema de información con acceso y/o exfiltración de datos personales, el envío de datos personales por error, la pérdida de dispositivos o documentación con datos personales, *malware* de tipo *ransomware* con exfiltración de datos, etc.

Es importante saber si los datos personales afectados estaban (total o parcialmente) cifrados de forma segura, anonimizados o protegidos de forma que sean ininteligibles para quien haya tenido acceso a dichos datos o lo pueda tener en el futuro. Si es así, las consecuencias de la brecha de confidencialidad quedan en gran medida mitigadas, reduciendo o incluso anulando los riesgos derivados del incidente.

2. Disponibilidad

Una brecha afecta a la disponibilidad de los datos personales cuando han estado inaccesibles de forma temporal o permanente para quien legítimamente debe poder tratarlos o acceder a ellos.

Esta situación puede ocurrir por sucesos que afecten a los datos personales en sí mismos o también por sucesos que afecten a los sistemas utilizados para su tratamiento. Por ejemplo, incluye casos de cifrado de datos personales o de los sistemas de información causado por malware de tipo ransomware, pérdida de documentación en papel con datos personales o la imposibilidad de acceder a un almacenamiento de datos (acceso físico o lógico).

Para el responsable del tratamiento es importante determinar si la disponibilidad se ha podido recuperar o está en vías de recuperación, dado que recuperar los datos y los sistemas de tratamiento es la vía para mitigar el daño que pueden producir este tipo de brechas de datos personales.

3. Integridad

Una brecha afecta a la integridad cuando se han alterado los datos personales de forma ilegítima y el tratamiento de esos datos personales puede causar un daño a los afectados.

Por ejemplo, un tercero ha modificado en la base de datos de la organización la información relativa a los datos bancarios de los empleados que se utilizan para el pago de las nóminas, o un alumno modifica las calificaciones en la base de datos de un centro educativo. Cuando se producen brechas de datos personales de integridad el responsable debe determinar si el tratamiento de los datos alterados ilegítimamente puede causar o ha causado algún daño a los afectados y en su caso si el daño se puede revertir.

[7] *Fuente: Guía para la notificación de brechas de datos personales de la AEPD.*

Ejemplos de clasificación de brechas de seguridad:

Suceso	Confidencialidad	Disponibilidad	Integridad
Revelación verbal no autorizada	X		
Documentación perdida, robada o en localización insegura	X	X	
Correo postal perdido o abierto	X	X	
Eliminación incorrecta de datos personales en papel		X	
Datos personales enviados por error de forma electrónica o papel	X		
Datos personales eliminados o destruidos		X	
Abuso de privilegios de acceso por parte de miembro (ej, empleado) para extraer, reenviar o copiar datos personales	X		
Datos personales residuales en dispositivos obsoletos	X		
Publicación no intencionada o autorizada	X		
Envío de correo electrónico a múltiples destinatarios sin copia oculta o en una lista de distribución visible	X		
Dispositivo perdido o robado	X	X	
Ciber incidente: Dispositivo ha sido cifrado / secuestro de la información	X	X	
Ciber incidente: Suplantación de identidad (phishing) / compromiso de cuenta de usuario o administrador	X	X	X
Ciber incidente: Acceso no autorizado a datos personales en un sistema de información ya sea corporativo o de un servicio en Internet	X	X	X
Incidencia técnica	X	X	X
Modificación no autorizada de datos			X
Datos personales mostrados al individuo incorrecto	X		

Anexo II - Guía Rápida de Actuación en caso de brecha de datos personales

Comillas es la responsable de todos los tratamientos de datos personales que se llevan a cabo en la Universidad pero también puede ser encargado del tratamiento en otros supuestos.

En cualquier caso, debe cumplir con la normativa europea y española de protección de datos, por lo que es importante la colaboración de todos para lograrlo. En caso de que detectes una brecha de datos personales, por favor, sigue los siguientes pasos:

1. Sospecho o tengo certeza de que **ha ocurrido una brecha de seguridad de datos personales**.

¿Qué es un dato personal?

Toda información sobre una **persona física identificada** o i**dentificable**.

Persona cuya identidad pueda determinarse mediante un identificador: nombre, datos de localización, DNI, teléfono, voz, imagen…

¿Qué es una brecha de seguridad?

Violación de seguridad que ocasione:
- destrucción
- pérdida
- alteración accidental o ilícita
- acceso o comunicación no autorizada

de datos personales transmitidos, conservados o tratados de otra forma.

2. **Comunico a mi responsable y a dpo@comillas.edu**. En caso de duda, si no tengo claro si lo ocurrido es una brecha de seguridad o no, también debo comunico igualmente. Además,
    - La comunicación debe ser lo más detallada posible.
    - Debo adjuntar y recopilar toda la información y documentos de lo sucedido.
3. Debo **informar de cualquier hecho nuevo** que tenga relación con lo sucedido.
4. En caso de que me indiquen que debo **tomar alguna medida**, la debo aplicar sin demora.
5. Tengo que estar **disponible para resolver cualquier consulta o duda** hasta que se cierre el incidente.

Anexo III - Normativa y guías que se han tenido en cuenta para redactar esta guía

Normativa:

- Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos, RGPD).

- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD).

Guías y directrices:

- Guía para la notificación de brechas de datos personales de la Agencia Española de Protección de Datos. https://www.aepd.es/es/documento/guia-brechas-seguridad.pdf

- Directrices 1/2021 sobre ejemplos de notificaciones de violaciones de la seguridad de datos personales del *European Data Protection Board.* https://edpb.europa.eu/system/files/2022-09/edpb_guidelines_012021_pdbnotification_adopted_es.pdf