Procedimiento para la gestión de violaciones de seguridad de datos personales

Referencia	25_Procedimiento de gestión de violaciones de seguridad_2_2023
Título de la *Norma*	Procedimiento para la gestión de violaciones de seguridad de datos personales
Ámbito geográfico	Nacional
Categoría	Procedimiento
Fecha de aprobación	16 de octubre de 2023
Órgano de aprobación	Comité de Compliance
Versión vigente	V2

Información importante sobre este documento	
Identificación del documento	Procedimiento para la gestión de violaciones de seguridad de datos personales
Referencia	25_Procedimiento de gestión de violaciones de seguridad_2_2023
Ámbito geográfico de aplicación	Nacional
Apartado de otras Normas que desarrolla	Código de Conducta
Normas que sustituye	Ninguna
Normas que deroga	Ninguna
Responsable principal de su vigilancia	*Patronato*
Órgano o Departamento que la propone	*Comité de Compliance*
Autor	*Comité de Compliance*
Órgano de aprobación	*Comité de Compliance*
Fecha de aprobación del texto vigente	16 octubre 2023
Fecha de aplicación	16 octubre 2023
Accesible en	Extra-Net

Control de Modificaciones

Versión	Fecha	Órgano de aprobación	Autor	Resumen de cambios
1	6 octubre 2021	Comité de Compliance	Comité de Compliance	
2	16 octubre 2023	Comité de Compliance	DPO	Revisión DPO

ÍNDICE

1. INTRODUCCIÓN Y OBJETO DEL DOCUMENTO

El Reglamento 2016/679 del Parlamento Europeo y del Consejo, 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 (en adelante RGPD) define, en su art. 4, una violación de seguridad 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*.

Conviene destacar que el RGPD, en inglés, habla de "brecha de datos personales", mientras que en castellano habla de "violación de la seguridad de los datos personales". Por todo ello, los conceptos de "brecha de datos personales", "brecha de seguridad" o "violación de la seguridad" deben entenderse sinónimos. En cualquier caso, se entiende por tales cualquier quiebra que se produzca sobre la disponibilidad, la integridad o la confidencialidad [1] de la información de carácter personal, aspectos que toda organización debe garantizar y sobre los cuales versarán las medidas de seguridad que se deben implementar.

Tenemos, por lo tanto, que una violación de seguridad será:

a) La destrucción, pérdida o alteración accidental o ilícita de datos personales (integridad y disponibilidad).

b) La comunicación o acceso no autorizados a los datos personales (confidencialidad).

El RGPD prevé que, ante una brecha o violación de seguridad, se deba informar a la autoridad de control competente, así como, en ciertos casos, a los interesados cuyo tratamiento de datos personales se ha visto afectado por la violación de seguridad. Se distingue así entre:

a) Notificación de una violación de la seguridad de los datos personales a la autoridad de control, que en España lo es la Agencia Española de Protección de Datos (AEPD).

[1] Así lo menciona igualmente el Grupo de Trabajo del Artículo 29 (GT29) en su Dictamen 03/2014 y en sus Directrices sobre Notificaciones de Violaciones de Seguridad de Datos Personales de fecha 3 de octubre de 2017.

b) Comunicación de una violación de la seguridad de los datos personales al interesado.

2. DEFINICIONES Y ACRÓNIMOS

2.1. DEFINICIONES

- **Autoridad de Control**: Autoridad pública independiente establecida dentro de un país del Espacio Económico Europeo y que vela por el cumplimiento de la normativa de protección de datos dentro de dicho territorio.

- **Categorías especiales de datos personales:** datos personales que revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación sindical, y datos genéticos, datos biométricos dirigidos a identificar de manera unívoca a una persona física, datos relativos a la salud o datos relativos a la vida sexual o la orientación sexual de una persona física.

- **Datos personales**: toda información sobre una persona física identificada o identificable («el interesado»); se considerará persona física identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona.

- **Datos de naturaleza penal**: Aquellos relativos a condenas e infracciones penales o a medidas de seguridad conexas (ej.: una orden de alejamiento) impuestas a una persona física.

- **Elaboración de perfiles, perfilado o perfilar**: Toda forma de tratamiento automatizado de datos personales consistente en utilizar datos personales para evaluar determinados aspectos personales de una persona física, en particular para analizar o predecir aspectos relativos al rendimiento profesional, situación económica, salud, preferencias personales, intereses, fiabilidad, comportamiento, ubicación o movimientos de dicha persona física.

- **Interesado**: Persona identificada o identificable cuyos datos personales son o van a ser tratados. Cualquier persona física cuyos datos personales son manejados por Fundación ACS. En el presente documento se pueden emplear también como sinónimos "afectado" o "solicitante".

- **Tratamiento** o **tratamiento de datos**: cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de datos personales, ya sea por procedimientos automatizados o no, como la recogida, registro, organización, estructuración, conservación, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción.

- **Responsable del tratamiento o responsable**: la persona física o jurídica, autoridad pública, servicio u otro organismo que, solo o junto con otros, determine los fines y medios del tratamiento; si el Derecho de la Unión o de los Estados miembros determina los fines y medios del tratamiento, el responsable del tratamiento o los criterios específicos para su nombramiento podrá establecerlos el Derecho de la Unión o de los Estados miembros.

- **Encargado del tratamiento o encargado**: la persona física o jurídica, autoridad pública, servicio u otro organismo que trate datos personales por cuenta del responsable del tratamiento.

2.2. ACRÓNIMOS

AEPD: Agencia Española de Protección de Datos.

CEPD: Comité Europeo de Protección de Datos.

DPD: Delegado de Protección de Datos.

EIPD: Evaluación de Impacto sobre Protección de Datos.

GT29: Grupo de Trabajo del Art. 29.

LOPD GDD: Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

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).

TID: Transferencia Internacional de Datos.

TJUE: Tribunal de Justicia de la Unión Europea.

TC: Tribunal Constitucional de España.

3. GESTIÓN DE UNA VIOLACIÓN DE SEGURIDAD DE DATOS PERSONALES

Fundación ACS ha confeccionado el presente procedimiento de gestión de incidencias y un formulario de registro de incidencias con el fin de que quede debidamente registrada cualquier incidencia que al producirse haya ocasionado alguna de las vulneraciones antes mencionadas.

Cualquier persona de Fundación ACS, desde el mismo momento en que tenga conocimiento de la existencia de una posible incidencia de seguridad, deberá comunicárselo al Responsable de Protección de Datos de la organización, quien deberá abrir la correspondiente investigación a fin de recabar toda la información posible concerniente a la incidencia y constatar si efectivamente se ha producido o no una violación de seguridad de datos personales.

Asimismo, el Responsable de Protección de Datos de Fundación ACS deberá evaluar la gravedad de la incidencia a fin de, entre otras cosas, determinar la necesidad de notificarla a la autoridad de control y, en su caso, comunicarla a los interesados afectados.

Para valorar el riesgo deberá atenderse al riesgo para los servicios asociados a los datos personales, si la identificación de los interesados es posible y si pueden existir perjuicios para sus derechos fundamentales, incluyendo daños físicos, reputacionales o posibilidad de que los datos sean usados por terceros para realizar acciones fraudulentas (phishing, suplantación de identidad…). Finalmente, deberá atenderse a si los daños son o no reversibles y si se puede mitigar el riesgo.

Si no se dispusiera de toda la información para realizar una correcta evaluación, ésta se llevará a cabo de manera provisional, de ser posible, con la información disponible en

ese momento y, una vez se tenga el resto de información o la información correcta, se procederá a realizar la evaluación definitiva sobre la gravedad de la incidencia.

En todo caso, la evaluación de la gravedad de la incidencia se llevará a cabo conforme a lo dispuesto en las Directrices del Grupo de Trabajo del art. 29 sobre Notificación de Violaciones de Datos Personales bajo el RGPD, así como a lo recogido en la Guía para la notificación de Brechas de datos personales de la Agencia Española de Protección de Datos.

Estas incidencias pueden afectar a cualquiera de los tratamientos de datos que Fundación ACS lleva a cabo y que se encuentran debidamente inventariados, con sus principales características, en su Registro de Actividades de Tratamiento.

La gestión de las incidencias y las debidas comunicaciones que proceda realizar (notificaciones a la autoridad y comunicaciones a los interesados) son cuestiones que se encuentran íntimamente ligadas al análisis de riesgos de los tratamientos de datos de Fundación ACS. Así pues, ante una brecha de seguridad, Fundación ACS debe acudir tanto al referido análisis de riesgos, así como al Registro de Actividades de Tratamiento a fin de, entre otras cosas, procurar:

- Valorar la gravedad de la vulneración de seguridad.
- Identificar la/s posible/s causa/s de la vulneración y factores o elementos involucrados en la misma.
- Identificar las categorías de interesados afectados por la violación de seguridad y las posibles consecuencias que puedan derivarse para ellos.
- Decidir qué medidas de seguridad cabe corregir o implementar.
- Evaluar el alcance de la vulneración y el perjuicio que pudiera ocasionarse a los interesados, así como si conlleva un alto riesgo para los interesados en función del impacto cuantificado para éstos en función de los tratamientos de datos afectados.
- Determinar si procede notificar a la autoridad de control y/o comunicar la brecha de seguridad a los interesados afectados.
- Identificar a los encargados del tratamiento que hayan podido verse involucrados en la brecha de seguridad.
- Identificar a posibles corresponsables y otros responsables a quienes se deba o convenga comunicar la violación de seguridad.

Fundación ACS documentará, con independencia de su gravedad y de si es necesario o no notificarla a la autoridad de control, toda violación de seguridad de los datos personales en un Registro de Incidencias en el que deben anotarse, como mínimo, los hechos relacionados con la brecha de seguridad, sus efectos y las medidas correctivas adoptadas.

Una vez el Responsable de Protección de Datos haya determinado qué medidas de seguridad deben implementarse, tanto para anular o mitigar en lo posible las consecuencias que para los interesados afectados se hayan podido derivar, como para evitar en lo posible que se repita en el futuro, las recomendará a la persona con capacidad decisoria al respecto para que decida finalmente al respecto y, en su caso, de las instrucciones precisas para la adopción de las medidas.

El Responsable de Protección de Datos de Fundación ACS hará seguimiento de las medidas propuestas y finalmente emitirá un Informe relativo a la incidencia en el que recogerá las fechas significativas, la averiguación llevada a cabo, la causa y el alcance de la incidencia, la gravedad de la misma, los tratamientos de datos afectados, las categorías de interesados afectados y las medidas propuestas y adoptadas.

4. NOTIFICACIÓN Y COMUNICACIÓN DE UNA VIOLACIÓN DE SEGURIDAD

4.1. NOTIFICACIÓN DE UNA VIOLACIÓN DE SEGURIDAD A LA AUTORIDAD DE CONTROL

¿Qué tipo de violaciones de seguridad deben notificarse a la autoridad de control?

Conforme al art. 33 RGPD debe notificarse a la Agencia Española de Protección de Datos, AEPD (u organismo que lo sustituya en el futuro) cualquier violación de seguridad que sea detectada por Fundación ACS, bien directamente bien por su puesta en conocimiento por parte de un tercero, siempre que:

- Dicha brecha de seguridad afecte a alguno de los tratamientos de datos que Fundación ACS esté llevando a cabo.
- Y conlleve un riesgo para los interesados afectados por los tratamientos de datos.

No será necesario notificar la violación de seguridad exclusivamente cuando no sea probable que constituya un riesgo significativo para los interesados. No se precisa que el riesgo que se derive para los interesados sea alto para resultar obligado a notificar la brecha a la autoridad de control.

A efectos prácticos, deberá notificarse cualquier incidente cuya severidad se haya valorado entre baja (incluido) y muy alta (de 2 a 5) de conformidad con el Anexo I: Criterios para evaluación de violación de seguridad.

En caso de que la violación de seguridad afecte a datos personales de interesados de distintos estados miembros de la UE, si Fundación ACS tuviera en dicho momento establecimientos en distintos países miembros, habría que determinar cuál es la autoridad de control principal a la que habrá que notificar la violación de seguridad de conformidad con lo dispuesto al respecto en las Directrices sobre Notificación de Violaciones de Datos Personales del Grupo de Trabajo del art. 29.

¿Cuándo debe notificarse?

La violación de seguridad debe notificarse a la autoridad de control sin dilación indebida, es decir lo antes que sea posible y a más tardar 72 horas después de que Fundación ACS

haya tenido constancia de ella. Si no puede realizarse en el plazo de 72 horas, cuando finalmente se realice la notificación, deberá expresarse los motivos por los que no se presentó en el indicado plazo. No obstante, el expresar las razones del retraso de la notificación no evita la sanción por incumplir el plazo legal.

Tener constancia de la violación de seguridad debe entenderse como tener un grado razonable de certeza de que ha ocurrido un incidente de seguridad que ha comprometido los datos personales.

Lo realmente importante es iniciar, a la mínima sospecha, las acciones inmediatas adecuadas para investigar un posible incidente a fin de determinar si los datos personales efectivamente han sido violados, y de ser así, para tomar medidas correctivas y notificar si es necesario.

¿Cómo se realiza la notificación?

A través del formulario en la Sede Electrónica de la AEPD, que permite notificar nuevas brechas de datos personales, o bien modificar una notificación durante los treinta días siguientes a su presentación para aclarar o completar la información inicialmente remitida.

El procedimiento puede realizarse a través de https://sedeagpd.gob.es/sede-electronica-web/vistas/formBrechaSeguridad/nbs/procedimientoBrechaSeguridad.jsf y deberá realizarse por persona que disponga de certificado de representante de la compañía, o bien, en caso de no ser posible, deberá aportarse documentación acreditativa de la autorización a representar a la compañía en este trámite, adjuntándola.

¿Debe notificarse a alguien más?

Para el caso de que Fundación ACS llegara a actuar como encargado de tratamiento para algún tercero, la violación de seguridad, si afecta a los tratamientos de datos realizados por cuenta de dichos terceros debe notificarse siempre a éstos, que serán quienes la comuniquen a la Autoridad de Control como responsables del tratamiento. Fundación ACS no comunicará directamente la brecha a la AEPD cuando la brecha de seguridad afecte exclusivamente a los tratamientos que se efectúan por cuenta de terceros para los que presta servicio.

Si la brecha afectara también a tratamientos de datos que Fundación ACS lleva a cabo para sus propias finalidades en calidad de responsable directo, se comunicará la brecha

tanto al tercero para el que se presten servicios como encargado, como a la AEPD en lo que se refiere a los tratamientos de datos que la Entidad lleva a cabo como responsable.

El encargado debe comunicar al responsable la existencia de la brecha de seguridad en los plazos indicados en el correspondiente Acuerdo de Encargo con cada uno de los responsables del tratamiento y, en todo caso, sin dilaciones indebidas desde que el encargado haya tenido conocimiento de ella. Conforme a las directrices de la AEPD, recogidas en su Guía para la notificación de brechas de datos personales, debe entenderse que no debe excederse el plazo de 72 horas desde la constancia.

Contenido de la notificación

La notificación de la violación de seguridad deberá contener la información requerida a través del formulario habilitado al efecto en la sede electrónica de la AEPD, y en todo caso como mínimo:

- Una descripción de la naturaleza de la violación de la seguridad de los datos personales, en la que deberá incluirse, siempre que ello sea posible:
    - Las categorías y el número aproximado de interesados afectados
    - Las categorías y el número aproximado de datos personales afectados.
- Si Fundación ACS hubiera designado a un Delegado de Protección de Datos (DPD), el nombre y los datos de contacto de éste y, de no tenerlo designado, otro punto de contacto con Fundación ACS a través del cual la autoridad de control y, en su caso, los responsables y encargados informados, puedan obtener más información.
- Las posibles consecuencias de la violación de la seguridad de los datos personales.
- Una descripción de las medidas adoptadas o propuestas por Fundación ACS para poner el mayor remedio posible a la violación de la seguridad de los datos personales, así como, en caso de ser posible, para mitigar los posibles efectos negativos.

Si no fuera posible facilitar la información simultáneamente, se presentará una notificación inicial. En la medida en que la comunicación no sea completa, la información se facilitará de manera gradual y sin dilación indebida. En todo caso, la información deberá completarse antes del plazo máximo de 30 días hábiles desde la notificación inicial de la brecha.

4.2. COMUNICACIÓN DE UNA VIOLACIÓN DE SEGURIDAD A LOS INTERESADOS

¿Qué tipo de violaciones de seguridad deben comunicarse a los interesados?

A diferencia del supuesto anterior, conforme al art. 34 RGPD debe comunicarse a los interesados titulares de los datos personales una violación de seguridad, siempre que:

- Dicha brecha de seguridad afecte a alguno de los tratamientos de datos que Fundación ACS lleve a cabo en relación con los datos de dichos interesados.
- Y además dicha violación conlleve un ALTO RIESGO para los interesados afectados por los tratamientos de datos.

Por lo tanto, para que sea obligatoria la comunicación a los interesados sobre la violación de seguridad es preciso que exista probabilidad de que el riesgo que se derive para ellos sea alto. Si es probable que el riesgo sea bajo o estándar y no alto, no será obligatoria esta comunicación.

A efectos prácticos, deberá notificarse cualquier incidente cuya severidad se haya valorado como alta o muy alta (entre 4 y 5) de conformidad con el Anexo I: Criterios para evaluación de violación de seguridad.

No será necesario enviar la comunicación a los interesados si se cumple alguna de las condiciones siguientes:

a) Los datos personales afectados por la brecha de seguridad han sido objeto de medidas de protección que los hagan ininteligibles para cualquier persona que no esté autorizada a acceder a ellos, como el cifrado.

b) Fundación ACS ha adoptado medidas ulteriores que garantizan que se ha eliminado la probabilidad de que se materialice el alto riesgo para los interesados afectados.

c) Supone un esfuerzo desproporcionado para Fundación ACS En este caso, se sustituirá la comunicación individual por una comunicación pública colectiva o una medida similar por la que pueda informarse de manera igualmente efectiva a los interesados.

¿Cuándo y cómo debe comunicarse?

La violación de seguridad debe comunicarse a los interesados sin dilación indebida desde que se tenga constancia de la misma y empleando en dicha comunicación un lenguaje claro y sencillo.

Tener constancia de la violación de seguridad debe entenderse como tener un grado razonable de certeza de que ha ocurrido un incidente de seguridad que ha comprometido los datos personales.

Lo realmente importante es iniciar, a la mínima sospecha, las acciones inmediatas adecuadas para investigar un posible incidente a fin de determinar si los datos personales efectivamente han sido violados, y de ser así, para tomar medidas correctivas y comunicar a los interesados si es necesario.

¿Debe comunicarse a alguien más?

Aparte de a los interesados afectados, la violación de seguridad deberá ser notificada a la autoridad de control competente y, en su caso, a otros responsables del tratamiento de datos, conforme se detalla en el epígrafe anterior.

Contenido de la comunicación

La comunicación de la violación de seguridad a los interesados deberá contener como mínimo:

- Si Fundación ACS hubiera designado a un Delegado de Protección de Datos (DPD), el nombre y los datos de contacto de éste y, de no tenerlo designado, otro punto de contacto con Fundación ACS a través del cual la autoridad de control y, en su caso, los responsables y encargados informados, puedan obtener más información.
- Las posibles consecuencias de la violación de la seguridad de los datos personales.
- Una descripción de las medidas adoptadas o propuestas por Fundación ACS para poner el mayor remedio posible a la violación de la seguridad de los datos personales, así como, en caso de ser posible, para mitigar los posibles efectos negativos.

Notificación a la autoridad	Comunicación a interesados
• Cuando entrañe un riesgo para los interesados. • Sin dilación indebida, a más tardar a las 72 horas. • Contenido: ✓ Descripción de la violación de seguridad ✓ Categorías y nº aprox. de interesados y tipos y nº aprox. de datos ✓ DPD u otro punto de contacto ✓ Posibles consecuencias ✓ Medidas adoptadas o propuestas.	• Cuando entrañe un ALTO riesgo para los interesados. Excepciones. • Sin dilación indebida y empleando un lenguaje claro y sencillo. • Contenido: ✓ DPD u otro punto de contacto ✓ Posibles consecuencias ✓ Medidas adoptadas o propuestas

Cuadro resumen de las notificaciones y comunicaciones de violaciones de seguridad

5. OBLIGACIONES POSTERIORES A LA NOTIFICACIÓN DE LA BRECHA

Una vez notificada la brecha de datos personales, el responsable ha de estar preparado para recibir y atender las comunicaciones de la AEPD. Estas notificaciones se remiten por vía electrónica a través del servicio *Notifica@*, recibiéndose en la Carpeta Ciudadana o la Dirección Electrónica Habilitada del Ministerio de Política Territorial y Función Pública.

Se entenderá que la notificación surte efectos en la fecha de recogida de la notificación electrónica.

Si no se accede a la notificación en diez días hábiles, se entenderá que se ha rechazado la notificación.

La AEPD puede solicitar información adicional, o bien ordenar la comunicación de la brecha a los interesados afectados, si considerara que el riesgo es alto.

En el caso de orden de comunicación a los afectados, deberá confirmarse, en el plazo de 30 días, salvo que en la orden se indique otra cosa, el haber ejecutado dicha comunicación. Esta confirmación deberá incorporar:

- Contenido de la comunicación a los afectados.
- Fecha o periodo de las comunicaciones a los afectados.
- Número de sujetos a los que se ha dirigido la comunicación.
- Medio utilizado.
- Justificación, en su caso, de haber optado por una comunicación pública.

La información adicional o la confirmación de comunicación a los interesados que, en su caso, deba remitirse a la AEPD, se enviará a través del registro electrónico, indicando que se trata de una "contestación a requerimiento".

6. ENLACES DE INTERÉS

En relación con las notificaciones a la autoridad de control y las comunicaciones a los interesados, el GT29 ha adoptado unas Directrices que resultan de gran utilidad para saber cómo proceder al respecto. Se encuentran disponibles en inglés y español, entre otros idiomas. Tituladas como *Guidelines on Personal data breach notification under Regulation 2016/679*, fueron adoptadas el 3 de octubre de 2017 y pueden consultarse en https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612052

Por su parte, la Agencia Española de Protección de Datos, ha emitido su Guía para la notificación de brechas de datos personales, que puede consultarse online en https://www.aepd.es/es/documento/guia-brechas-seguridad.pdf que aporta en detalle un procedimiento para la gestión de estas brechas así como un modelo de notificación a la autoridad de control y ejemplos ilustrativos de brechas de seguridad.

7. MODELOS Y FORMULARIOS

7.1. MODELO DE REGISTRO DE INCIDENCIAS

Registro de incidencias de datos personales

Nº de incidencia	[Por ejemplo 001/2018]
Fechas relevantes	Fecha de la producción de la incidencia: Fecha del primer conocimiento: Fecha de constancia o confirmación:
Descripción detallada de la violación de datos personales	

Archivos relacionados	
Tipo de brecha (marcar a qué afecta)	☐ Integridad ☐ Disponibilidad ☐ Confidencialidad
Severidad	☐ Muy Baja ☐ Baja ☐ Media ☐ Alta ☐ Muy Alta
Fecha y hora en la que se estima se produjo la violación de seguridad	
Tratamientos de datos afectados por la violación de seguridad	
Categorías de interesados afectados y número aproximado de interesados afectados	
Categorías especiales de datos afectadas	
Facilidad de identificación de las personas	☐ Muy Baja ☐ Baja ☐ Media ☐ Alta ☐ Muy Alta
Consecuencias que puede producir	
Medidas propuestas y estado	

Notificación a la Autoridad de Control	[Indicar si procede la notificación o no, y en su caso por qué no procede o la fecha en que se produce la notificación]
Comunicación a los interesados	[Indicar si procede la comunicación o no, y en su caso por qué no procede o la fecha en que se produce la comunicación]
Fecha de cierre de la incidencia	[Fecha en que la incidencia ha quedado solventada y se archiva]

[Empléese el cuadro anterior para cada incidencia que se detecte]

7.2. NOTIFICACIÓN DE LA VIOLACIÓN A LA AUTORIDAD DE CONTROL SI NO PUDIERA REALIZARSE A TRAVÉS DE SEDE ELECTRÓNICA

Fundación ACS

Avda. Pío XII, 102, CP. 28036, Madrid

En Avda. Pío XII, 102, CP. 28036, Madrid, a ___ de _____ de _____

A la Att. de Don/Doña _____

Agencia Española de Protección de Datos

Por la presente, en cumplimiento de lo dispuesto en el art. 33 del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, Reglamento General de Protección de Datos (RGPD), se pone en conocimiento de esta Autoridad que en el día _____ esta empresa ha tenido conocimiento de la existencia de una violación de seguridad de datos personales en relación con ciertos tratamientos de datos respecto a los que actuamos en calidad de _____[indicar lo que proceda: responsables/encargados]_____

Tras llevar a cabo las acciones inmediatas de investigación pertinentes, les notificamos la siguiente información relativa a la mencionada violación de seguridad:

Nº de incidencia	[Por ejemplo 001/2018]
Fechas relevantes	Fecha de la producción de la incidencia: Fecha del primer conocimiento: Fecha de constancia o confirmación:
Descripción detallada de la violación de datos personales	
Archivos relacionados	
Tipo de incidencia (marcar a qué afecta)	☐ Integridad ☐ Disponibilidad ☐ Confidencialidad
Severidad	☐ Muy Baja ☐ Baja ☐ Media ☐ Alta ☐ Muy Alta
Fecha y hora en la que se estima se produjo la violación de seguridad	
Tratamientos de datos afectados por la violación de seguridad	
Categorías de interesados afectados y número aproximado de interesados afectados	

Categorías especiales de datos afectadas	
Facilidad de identificación de las personas	☐ Muy Baja ☐ Baja ☐ Media ☐ Alta ☐ Muy Alta
Consecuencias que puede producir	
Medidas propuestas y estado	
Notificación a la Autoridad de Control	[Indicar si procede la notificación o no, y en su caso por qué no procede o la fecha en que se produce la notificación]
Comunicación a los interesados	[Indicar si procede la comunicación o no, y en su caso por qué no procede o la fecha en que se produce la comunicación]
Fecha de cierre de la incidencia	[Fecha en que la incidencia ha quedado solventada y se archiva]

Para más información que puedan precisar, así como para cualquier colaboración o comunicación adicional que podamos prestar desde Fundación ACS, pueden contactar con nosotros a través de la dirección postal Avda. Pío XII, 102, 28036 Madrid, teléfonos 91 343 9573 / 91 343 9574 y correo electrónico info@fundacionacs.com.

En_____, a _____ de _____ de 2.0__.

Fdo.

7.3. COMUNICACIÓN DE LA VIOLACIÓN A LOS INTERESADOS

Fundación ACS

Avda. Pío XII, 102, CP. 28036, Madrid

En [Dirección], a ___ de _____ de _____

A la Att. de Don/Doña _____

[Dirección completa]

Desde Fundación ACS hemos estado siempre altamente sensibilizados con la importancia del tratamiento de sus datos personales y a tal efecto hemos adoptado y controlado de forma continua y hemos revisado periódicamente, las medidas de seguridad, técnicas y de organización, necesarias para proteger sus datos personales con altos niveles de garantía. Sin embargo, lamentablemente ningún sistema de seguridad es infalible y el día _____ esta empresa ha tenido conocimiento de la existencia de una violación de seguridad de datos personales de la que puede resultar afectado.

Tras llevar a cabo las acciones inmediatas de investigación pertinentes, se aprecia que las consecuencias que podrían derivarse para usted a raíz de la indicada violación de seguridad consisten en:

1. _____
2. _____
3. _____

Le informamos de que, ante este suceso, hemos actuado con la rapidez y diligencia debidas para, constatar la existencia de la violación de seguridad y determinar el alcance de la misma, así como en adoptar, de manera inmediata, las siguientes medidas para corregir esta situación y para mitigar sus posibles efectos:

1. _____

2. _____

3. _____

Asimismo, le indicamos que estamos en trámite de implementar, de manera adicional, las siguientes medidas que se consideran igualmente apropiadas en atención a la naturaleza de la violación de seguridad de datos personales, a las características de los tratamientos de datos afectados y teniendo en cuenta las medidas de seguridad que Fundación ACS ya tenía implementadas con anterioridad a la producción de esta brecha de seguridad:

1. _____

2. _____

3. _____

En todo caso, le pedimos su colaboración conminándole a que, por su parte, proceda a realizar las siguientes acciones de protección complementarias:

1. _____

2. _____

3. _____

Confiamos en que, con la adopción de todas estas medidas, no se materialice ningún perjuicio para usted. En caso de producirse el mismo, o si tuviera usted información adicional que considere pueda sernos de utilidad en la investigación y gestión de esta violación de seguridad, le rogamos se ponga en contacto con nosotros a la mayor brevedad a fin de poder atender cuanto sea preciso para la minoración de los posibles efectos.

Igualmente, para más información que puedan precisar, así como para cualquier colaboración o comunicación adicional que podamos prestar desde Fundación ACS, pueden contactar con nosotros a través de la dirección postal Avda. Pío XII, 102, 28036 Madrid, teléfonos 91 343 9573 / 91 343 9574 y correo electrónico info@fundacionacs.com.

En_____, a _____ de _____ de 2.0__.

Fdo.

7.4. NOTIFICACIÓN A OTROS RESPONSABLES O ENCARGADOS

Fundación ACS

Avda. Pío XII, 102, CP. 28036, Madrid

En [Dirección], a ___ de _____ de _____

A la Att. de Don/Doña _____

Desde Fundación ACS hemos estado siempre altamente sensibilizados con la importancia del tratamiento de los datos personales que llevamos a cabo para poder prestarle el servicio encargado en virtud del contrato de _____ suscrito con ustedes el día _____. A tal efecto, como saben, hemos adoptado y controlado de forma continua y hemos revisado periódicamente, las medidas de seguridad, técnicas y de organización, necesarias para proteger los datos personales de los que ustedes son responsables con altos niveles de garantía.

Sin embargo, lamentablemente ningún sistema de seguridad es infalible y el día _____ esta empresa ha tenido conocimiento de la existencia de una violación de seguridad de datos personales en relación con tratamientos de datos en los que intervenimos en calidad de encargado/subencargado del tratamiento suyo.

En consecuencia, de conformidad con lo dispuesto en el art. 34 del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, Reglamento General de Protección de Datos (RGPD) y tras llevar a cabo las acciones inmediatas de investigación pertinentes, les aportamos, para su debido conocimiento y diligencia, la siguiente información relativa a la mencionada violación de seguridad:

INFORMACIÓN SOBRE VIOLACIÓN DE SEGURIDAD DE DATOS PERSONALES

Nº de incidencia	
Fecha de detección	
Tipo de incidencia	☐ Integridad ☐ Disponibilidad ☐ Confidencialidad
Descripción detallada de la violación de seguridad	
Fecha y hora en la que se estima se produjo la violación de seguridad	
Tratamientos de datos afectados por la violación de seguridad	
Categorías de interesados afectados y número aproximado de interesados afectados	**Categorías:** **Nº aprox. interesados:**
Categorías especiales de datos afectadas	
Facilidad de identificación de las personas	☐ Muy Baja ☐ Baja ☐ Media ☐ Alta ☐ Muy Alta
Consecuencias que puede producir	
Medidas propuestas y ya adoptadas	

Medidas propuestas en proceso de adopción	
Medidas que se proponen para que sean implementadas por __[DESTINATARIO DE LA NOTIFICACIÓN]___	

Como siempre, estaremos encantados de colaborar con ustedes y prestarles cuanta ayuda esté en nuestra mano a fin de reducir las consecuencias que puedan derivarse de la mencionada violación de seguridad.

Para más información que puedan precisar, así como para cualquier colaboración o comunicación adicional que podamos prestar desde Fundación ACS, pueden contactar con nosotros a través de la dirección postal Avda. Pío XII, 102, 28036 Madrid, teléfonos 91 343 9573 / 91 343 9574 y correo electrónico info@fundacionacs.com.

En_____, a _____ de _____ de 2.0__.

Fdo.

8. ANEXOS

8.1. Anexo I: Criterios para la evaluación de violación de seguridad

I: Indicador de Severidad (1 a 5, siendo 1 el valor de menor severidad y 5 el de mayor severidad).

TIPO DE BRECHA (TB) *NC = No computa en la valoración	**I**
No intencionada	1
Intencionada con fin distinto a provocar un daño a los interesados y/o terceros	2
Intencionada que persigue hacer daño a un tercero distinto a los interesados	3
Intencionada que persigue hacer daño a los propios interesados	4
Intencionada que persigue hacer daño a los propios interesados y a un/os tercero/s	5
Se desconoce	NC*
NÚMERO DE INTERESADOS AFECTADOS (IA)	**I**
De 0 a 250	1
De 251 a 1.000	2
De 1.001 a 5.000	3
De 5.001 a 50.000	4
Más de 50.000	5
TIPO DE DATOS COMPROMETIDOS (TD)	**I**

Datos de escasa identificación (nombre, apellidos, correo electrónico, teléfono…)	1
Datos de escaso riesgo: más datos identificativos y de contacto, de educación, familiares, profesionales, biográficos, de asociación o similares	2
Datos de comportamiento: localización, tráfico, hábitos y preferencias	3
Datos financieros: transacciones, posiciones, ingresos, cuentas, facturas	4
Datos sensibles: de categorías especiales y/o relativos a infracciones y condenas penales	5
VOLUMEN DE DATOS DE CADA INTERESADO (VD)	**I**
Muy bajo	1
Bajo	2
Medio	3
Alto	4
Muy alto	5
FACILIDAD DE IDENTIFICAR A LOS INTERESADOS A PARTIR DE LA INFORMACIÓN REVELADA (FI)	**I**
Muy bajo	1
Bajo	2
Medio	3
Alto	4
Muy alto	5
TIPO DE INTERESADOS POR SU VULNERABILIDAD, siempre que ello les exponga a un mayor riesgo (TI) à Mín. 1 y Máx. 5	**I**

Personas bajo amenaza (testigos protegidos, víctimas de violencia de género, víctimas de bullying…)	5
Personas vulnerables (personas con discapacidad, solicitantes de asilo o refugio, excarcelados…) y personas que pueden sufrir algún tipo de discriminación (por razón de sexo, raza, religión, preferencias sexuales, etc.)	4
Personas con funciones sensibles a la seguridad (miembros de fuerzas y cuerpos de seguridad, funcionarios de prisiones, personal de instituciones psiquiátricas…), Celebridades, políticos y otras personas con relevancia pública o noticiable.	3
Menores	2
Ninguna de las categorías anteriores	1
LA INFORMACIÓN REVELADA PERMITE REALIZAR PROFILING DE LOS INTERESADOS (PRF) à Mín. 1 y Máx. 5	I
No	1
Leve	2
Medio	3
Alto	4
Muy alto	5
TIPO DE CONSECUENCIAS PARA LOS INTERESADOS (SC)	I
No concurre ninguno de los restantes supuestos de este apartado	1
Las personas no se verán afectadas o pueden encontrar algunos inconvenientes que superarán sin ningún problema (tiempo de reingreso de información, molestias, irritaciones, etc.).	2
Las personas pueden encontrar inconvenientes importantes, que podrán superar a pesar de algunas dificultades (costos adicionales, denegación de acceso a	3

servicios comerciales, miedo, falta de comprensión, estrés, dolencias físicas menores, etc.).	
Las personas pueden enfrentar consecuencias importantes, que deberían poder superar aunque con serias dificultades (malversación de fondos, listas negras de los bancos, daños a la propiedad, pérdida de empleo, citación judicial, suplantación de la identidad con consecuencias jurídicas o similares o detrimento de su dignidad, daño a su honor o reputación, empeoramiento de la salud, etc.).	4
Las personas pueden enfrentar consecuencias significativas, o incluso irreversibles, que no pueden superar (exclusión o marginación social, dificultades financieras tales como deudas considerables o incapacidad para trabajar, dolencias psicológicas o físicas a largo plazo, muerte, etc.).	5
CARACTERÍSTICAS PROPIAS DE LA ENTIDAD QUE SUFRE LA BRECHA (CE)	**I**
El riesgo para los afectados no incrementa de ninguna manera por las características de la propia entidad.	1
El riesgo para los afectados se incrementa en un grado bajo por las características de la propia entidad.	2
El riesgo para los afectados se incrementa en un grado medio por las características de la propia entidad.	3
El riesgo para los afectados se incrementa en un grado alto por las características de la propia entidad.	4
El riesgo para los afectados se incrementa en un grado muy alto por las características de la propia entidad.	5

Entre todos los criterios se obtendrá la media de severidad (fórmula: [(TB+IA+TD+VD+FI+TI+PRF+SC+CE)/nº de criterios computables]) y podrá añadirse algún factor de corrección, agravante o atenuante, que pueda concurrir dependiendo de cada caso. En función del resultado, el ciberincidente se deberá notificar o no a la autoridad de control de protección de datos (en España la AEPD) y a los interesados, conforme se indica en el siguiente cuadro:

1	**Severidad muy baja** (No requiere notificar a la autoridad de control ni comunicar a interesados)
2	**Severidad baja** (A partir de este valor requiere notificar a la autoridad de control pero no comunicar a los interesados)
3	**Severidad media** (Requiere notificar a la autoridad de control pero no comunicar a los interesados)
4	**Severidad alta** (A partir de este valor requiere notificar a la autoridad de control y comunicar a los interesados)
5	**Severidad muy alta** (Requiere notificar a la autoridad de control y comunicar a los interesados)