ACUERDO POR EL QUE SE APRUEBA LA NORMATIVA PARA LA GESTIÓN DE BRECHAS DE SEGURIDAD DE LA UNIVERSITAT POLITÈCNICA DE VALÈNCIA

Aprobada por Consejo de Gobierno de 25 de julio de 2024

Editor: Secretaria General / UPV · D.L.: V-5092-2006 · ISSN: 1887-2298 · www.upv.es/secgen

PREÁMBULO

Con la entrada en vigor del 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 y la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, las entidades que tratan datos personales se han visto en la obligación de establecer procedimientos y protocolos para la gestión y notificación de los incidentes y brechas de seguridad que supongan un riesgo para los derechos y libertades de las personas físicas.

Así las cosas, la Universitat Politècnica de València (en adelante "UPV"), en el desarrollo de la "Normativa de Seguridad" ha decidido desarrollar la presente Normativa para la Gestión de Brechas de Seguridad para la correcta gestión de los incidentes que afecten a datos personales cuyo responsable sea la propia Universitat.

El objetivo de esta normativa es desarrollar el procedimiento operativo por parte de la Universitat en relación con la gestión y notificación de todos aquellos eventos relacionados con privacidad. Es por ello que constituye una normativa interna de obligado cumplimiento para todo el personal de la UPV, a partir de la fecha de su aprobación.

De forma general, y para alinear la UPV con la legislación (artículo 33 del RGPD), el tiempo máximo de comunicación a la autoridad de control (Agencia Española de Protección de Datos en España) de una violación de privacidad no debe de superar las 72 horas desde el momento en el que se identifica la violación de privacidad. Dicha notificación, la debe llevar a cabo el Delegado de Protección de Datos nombrado en la Universitat.

En el presente procedimiento se regulan aspectos fundamentales de la gestión de brechas de seguridad, tales como: (i) el ámbito de aplicación del procedimiento, (ii) la identificación y registro inicial de los eventos, (iii) su catalogación conforme a la definición de brecha de seguridad, (iv) su gestión y tratamiento del riesgo que representa para los derechos, (v) en su caso, la notificación de la brecha a la autoridad de control competente, (vi) en su caso, la notificación de la brecha a los afectados, (vii) así como el resto de obligaciones derivadas para todos los sujetos obligados por el presente procedimiento.

En la creación del presente documento se han visto implicadas las principales áreas para la gestión de los incidentes y brechas de seguridad, entre ellas: el Área Jurídica y de Delegación de Protección de Datos, el Área de Sistemas de Información y Comunicaciones (ASIC) y, en aplicación del concepto de "Top-Down" para la gestión de las políticas de compliance y cumplimiento normativo, por los más altos órganos de dirección de la Universitat.

Artículo. 1.- Objeto

El objetivo de esta norma es definir y establecer el procedimiento mediante el cual se deben identificar, catalogar, resolver y/o escalar todas aquellas entradas relacionadas con eventos en los que se vean implicados "datos personales".

Artículo 2.- Definiciones

1.“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.

2.“Tratamiento”: 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.

Artículo 3.- Ámbito de Aplicación

Este documento se aplica a todas las actividades de la UPV en el ámbito de la obtención, tratamiento y comunicación de datos de carácter personal.

1. Este documento es de obligado cumplimiento para toda la comunidad universitaria o personal externo que tenga acceso a los datos de carácter personal que son tratados por la Universitat. Las normas internas contenidas en el presente documento se tienen que poner en conocimiento de toda la comunidad con acceso a datos de carácter personal o con acceso a los sistemas de información de la Universitat, para que sepan cómo actuar ante la detección de una posible brecha de seguridad.

2. El presente documento aplica a todos los sistemas de información que dispone la Universitat en sus distintos centros de trabajo, conforme a lo establecido en el “Anexo I - Apartado 1” de la presente normativa.

Artículo 4.- Comunicación de los incidentes

1. En el momento en que un usuario del sistema de la información identifique un evento, incidente o violación de seguridad, deberá notificarlo en el plazo de 24 horas al Delegado de Protección de Datos y a la unidad de incidentes del ASIC en los datos indicados en el “Anexo I – Apartado 2” de la presente normativa.

2. La comunicación deberá realizarse por correo electrónico, indicando de forma detallada la situación detectada, las consecuencias que ha producido la misma y las actuaciones llevadas a cabo por parte del usuario.

3. Para contactar con la unidad de incidentes, el usuario podrá utilizar también los medios de contacto disponibles en el “Anexo I – Apartado 2” de la presente normativa.

Artículo 5.- Identificación y registro inicial de los incidentes de seguridad.

1. La identificación de una entrada de privacidad puede ocurrir por varios actores diferenciados, como, por ejemplo: un empleado que solicita la apertura de una entrada, Seguridad Corporativa, Gestión de Personal, por un 3º de confianza especializado, etc.

2. Independientemente del actor que identifique el caso, el evento será registrado por el personal del ASIC en el registro de incidencias como incidente de seguridad, conformando el punto centralizador del incidente, en el que se incorporará la información inicial del evento y se catalogará inicialmente de forma homogénea. Los roles y responsabilidades en este sentido serán designados por el ASIC en la correspondiente instrucción o documento.

3. Si el incidente afecta a datos personales, el ASIC deberá informar de manera inmediata al Delegado de Protección de Datos y a la Directora del Área Jurídica y Delegación de Protección de Datos, para evaluar la afectación de los derechos y libertades de los interesados y valorar la comunicación a la Agencia Española de Protección de Datos (AEPD) y a los interesados.

La centralización en el ASIC como equipo centralizador de primer nivel permitirá la implicación y coordinación de los diferentes departamentos requeridos para resolver cada uno de los eventos de forma eficaz según su naturaleza.

4. Los registros mínimos para cumplimentar en un incidente de seguridad con afectación a datos personales serán:

a) Fecha y hora de la detección.
b) Detección. [empleado, colaborador, 3º de confianza, externo].
c) Naturaleza del evento de seguridad de los datos personales.
d) Descripción breve.
e) Sistema afectado.
f) Tipo y número aproximado por categoría de interesados afectados [menores, empleados, directivos, afiliados a sindicatos, etc.…].
g) Categorías y número aproximado de registros de datos personales afectados [DNI, nombre y apellidos, direcciones, matrículas, credenciales, etc.…].
h) Descripción de las posibles consecuencias del evento de privacidad.
i) Descripción de las medidas adoptadas para contener y mitigar el evento.
j) Criticidad en relación con privacidad [se desarrolla en el siguiente capítulo].
k) Estado actual del evento.
l) Procedimiento de resolución [si aplicase].
m) Fecha de resolución [si aplicase].

5. Es posible que durante el primer registro del evento no se disponga de toda la información descrita, en cuyo caso deberá de solicitarse más información y la investigación del evento para poder cumplimentar al menos con información aproximada los campos requeridos.

Artículo 6.- Catalogación y escalado de eventos de privacidad

1. Una vez registrado la entrada de privacidad y recopilada la información disponible en primera instancia, se realizará una primera catalogación. Se considerará brecha de seguridad "todo Incidente de Seguridad o 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 autorizado a dichos datos", según lo indicado en el artículo 4.1 del Reglamento 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.

2. Se establecen tres grandes categorías para las entradas de privacidad, a saber: evento, incidente y violación. Esta última categoría referente a la violación de privacidad, se subdivide asimismo en dos categorías según la afección que suponga a las libertades y derechos de los afectados.

3. Se entenderá por violación de seguridad de datos de carácter personal, 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 todo caso, cualquier entrada que afecte o impacte en las dimensiones de la seguridad (Confidencialidad, Integridad o Disponibilidad) debe ser considerado al menos como un evento de privacidad siempre que afecte a un sistema de información que contenga datos de carácter personal.

Los criterios que debe de cumplir una entrada para ser categorizado como tal en la Universitat se definen en el Anexo II de la presente normativa.

Artículo 7.- Gestión y tratamiento de entradas

1. Según la clasificación de la entrada, el seguimiento y tratamiento de la misma variará, dependiendo de si nos encontramos ante un evento, una incidencia o una violación.

2. Para la gestión de los "eventos", el tratamiento y resolución habitual de la entrada realizado por los procedimientos estándar del ASIC. El responsable de Seguridad reportará al Delegado de Protección de Datos la existencia del evento mediante un informe detallado tan pronto tenga constancia de la afectación de datos personales.

3. Para la gestión de las "incidencias", el tratamiento y resolución habitual de la entrada realizado por los procedimientos estándar del ASIC. El responsable de Seguridad reportará al Delegado de Protección de Datos la existencia del evento mediante un informe detallado tan pronto tenga constancia de la afectación de datos personales. Tanto el ASIC como el Delegado de Protección de Datos, podrán iniciar una investigación sobre el incidente de cara a obtener más información sobre el mismo de forma que puedan adoptarse las medidas de protección adicionales que se consideren, así como la posible notificación de la incidencia a la AEPD.

4. Para la gestión de las “violaciones”, el tratamiento y resolución habitual de la entrada realizado por los procedimientos estándar del ASIC. El responsable de Seguridad reportará al Delegado de Protección de Datos la existencia del evento mediante un informe detallado tan pronto tenga constancia de la afectación de datos personales. Tanto el ASIC como el Delegado de Protección de Datos, podrán iniciar una investigación sobre el incidente de cara a obtener más información sobre el mismo de forma que puedan adoptarse las medidas de protección adicionales que se consideren, así como la posible notificación de la incidencia a la AEPD.

Artículo 8.- Notificación a las autoridades

1. Cualquier entrada categorizada como “Violación de Privacidad” será notificada a la Agencia Española de Protección de Datos o autoridad de control competente, por el Delegado de Protección de Datos de la Universitat. La notificación se realizará a más tardar 72 horas después de que se haya tenido constancia de ella.

2. Si la incidencia se ha producido en el sistema de información de la Universitat, se le comunicará al Delegado de Protección de Datos en un plazo máximo de 24 horas desde que se ha tenido constancia de la incidencia.

3. Si la incidencia se ha producido en el sistema de información de un tercero, encargado del tratamiento de la Universitat, este tercero le comunicará a la Universitat la incidencia en un plazo máximo de 24 horas desde que tuvo constancia y, seguidamente, la Universitat se lo comunicará al Delegado de Protección de Datos en un plazo de 24h adicionales. La comunicación al Delegado de Protección de Datos se realizará mediante el canal correspondiente indicado en el Anexo I de esta norma.

4. Asimismo, el Delegado de Protección de Datos de la Universitat, y bajo su propio criterio, podrá notificar aquellas entradas catalogadas como “Incidente” que considere oportunas. El criterio general para estos casos será el de notificar cualquier entrada que pueda suponer un riesgo para los derechos y las libertades de las personas físicas.

5. En la notificación se deberá de incluir al menos la siguiente información:

a) Describir la 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) Comunicar el nombre y los datos de contacto del Delegado de Protección de Datos o de otro punto de contacto en el que pueda obtenerse más información.

c) Describir las posibles consecuencias de la violación de la seguridad de los datos personales.

d) Describir las medidas adoptadas o propuestas por el responsable del tratamiento 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.

e) En caso de que no fuese posible facilitar toda la información en un primer reporte, podrán realizarse notificaciones graduales que incorporen la información requerida según se disponga de ella.

6. La notificación se realizará en la sede electrónica de la Agencia Española de Protección de Datos. A modo de contingencia, en caso de no estar disponible el servicio electrónico de la Agencia Española de Protección de Datos, se deberá contactar con esta por cualquiera de los medios facilitados en el Anexo I de esta norma, para acordar el canal alternativo por el que realizar la notificación.

Artículo 9.- Notificación a los interesados

1. Cualquier "Violación de Privacidad" categorizada como "Crítica" será notificada a los afectados previa revisión del contenido de la notificación por parte del Delegado de Protección de Datos. La notificación se realizará lo antes posible una vez que se haya tenido constancia del alcance y afectación a los derechos y libertades de los interesados.

2. La notificación describirá en un lenguaje claro y sencillo la naturaleza de la violación de privacidad y contendrá al menos la siguiente información:

a) Nombre y los datos de contacto del Delegado de Protección de Datos o de otro punto de contacto en el que pueda obtenerse más información.

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

c) Describir las medidas adoptadas o propuestas por el responsable del tratamiento 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.

3. Se establecen las siguientes excepciones a la obligatoriedad de la comunicación de las entradas catalogadas como "Violación de Privacidad" definida como "Crítica" a los interesados en caso de cumplirse alguna de las siguientes condiciones:

a) Se han adoptado medidas de protección técnicas y organizativas apropiadas de forma que puede asegurarse que la información personal es ininteligible para cualquier persona que no esté autorizada para acceder a la información (P. ej.: cifrado).

b) El responsable del tratamiento ha tomado medidas ulteriores que garanticen que ya no exista la probabilidad de que se concretice el alto riesgo para los derechos y libertades de los interesados.

c) Suponga un esfuerzo desproporcionado. En este caso, se optará en su lugar por una comunicación pública o una medida semejante por la que se informe de manera igualmente efectiva a los interesados.

Editor: Secretaria General / UPV · D.L.: V-5092-2006 · ISSN: 1887-2298 · www.upv.es/secgen

Artículo 10.- Comunicación a empleados y colaboradores.

1. Cualquier entrada que suponga una violación de privacidad catalogada como “Crítica” será notificada a los empleados y colaboradores por el ASIC, previa revisión del contenido de la notificación por parte del Delegado de Protección de Datos.

2. La notificación describirá en un lenguaje claro y sencillo la naturaleza de la violación de privacidad, así como el posicionamiento corporativo en relación con la violación ocurrida.

Artículo 11.- Contención y mitigación

1. En caso de requerirse la contención y mitigación técnica, la entrada se identificará adicionalmente como “Ciberincidente”, con lo que se gestionará su tratamiento según el procedimiento estándar de Seguridad.

2. En caso de tratarse de un caso de excepcional gravedad, podrá solicitarse la invocación del procedimiento de gestión de crisis o plan de continuidad.

Artículo 12.- Incumplimiento de la Normativa

1. El responsable de seguridad de la información, en el ejercicio de sus funciones, ante un posible incumplimiento de la presente normativa que pueda suponer un perjuicio grave para la información o los datos personales tratados por la UPV, podrá, previa autorización del Rector, proceder a la suspensión cautelar del tratamiento de datos realizado así como al bloqueo temporal de sistemas, cuentas o accesos a la red de forma preventiva, con el fin de garantizar el buen funcionamiento de los servicios de la institución, sin perjuicio de los procedimientos administrativos y disciplinarios que correspondan en su caso.

2. En los demás supuestos de incumplimiento, se advertirá del hecho al infractor. En caso de que el usuario no responda o ignore la advertencia, el responsable de Seguridad de la Información de la Universitat podrá iniciar los procedimientos administrativos y disciplinarios que correspondan en su caso.

Todo ello sin perjuicio de iniciar las acciones judiciales civiles y, en su caso, penales que pudieran corresponder, en relación con las personas presuntamente implicadas en dicho incumplimiento.

La Universitat Politècnica de València pondrá en conocimiento de la autoridad judicial y las Fuerzas y Cuerpos de Seguridad del Estado aquellas infracciones que pueden ser constitutivas de delito.

Disposición final única. Entrada en vigor.

Esta Normativa entrará en vigor el mismo día de su publicación en el Butlletí Oficial de la Universitat Politècnica de València (BOUPV).

Editor: Secretaria General / UPV · D.L.: V-5092-2006 · ISSN: 1887-2298 · www.upv.es/secgen

ANEXO I – Datos de contacto

1. Centros de Trabajo de la UPV:
   a) Campus Vera, ubicado en Camino de Vera s/n, CP 46022 – Valencia (España)
   b) Campus Alcoy, ubicado en Plaza de Ferrándiz y Carbonell s/n, CP 03801 – Alcoy (Alicante-España)
   c) Campus Gandía, ubicado en C/ Paranimf 1, CP 46730 – Grao de Gandia – (València - España)
   d) Cualquier otro centro de trabajo físico que se establezca en el territorio de actuación de la entidad.

2. Datos de contacto para la comunicación de los incidentes:
   a) Delegado de Protección de Datos: dpd@upv.es
   b) Unidad de incidentes del ASIC:
   - Correo electrónico: incidentes@upv.es.
   - Teléfono: Si el usuario es persona externa a la comunidad, deberá llamar al +34 963877750; y si es personal de la Universitat, deberá marcar la extensión 77750.
   - Aplicación Gregal, disponible para la comunidad universitaria y externos.

3. Datos de contacto de la Agencia Española de Protección de Datos:
   a) Teléfono: 901 100 099 - 912 663 517
   b) Dirección postal: C/ Jorge Juan, 6. 28001 – Madrid, España.

Editor: Secretaria General / UPV · D.L.: V-5092-2006 · ISSN: 1887-2298 · www.upv.es/secgen

ANEXO II – Cuadro de categorización de los eventos de seguridad.

Categoría	Criticidad RGPD	Descripción del nivel	Ejemplos de perjuicio potencial al usuario
Evento	Despreciable	El impacto sobre las personas afectadas es muy reducido. Los posibles inconvenientes pueden ser subsanados fácilmente.	- Pérdida de tiempo por necesidad de repetir procedimientos. - Pérdida de confidencialidad de un dato personal aislado.
Incidente	Limitado	El impacto sobre las personas afectadas está acotado. Los posibles inconvenientes pueden ser subsanados, aunque requiere un esfuerzo económico y trabajo adicional.	- Perjuicio económico menor. - Pérdida de confidencialidad de varios datos personales por afectado. - Perjuicio social potencial menor.
Violación de privacidad	Importante	El impacto sobre las personas afectadas es elevado. Los posibles inconvenientes son difícilmente subsanables ya que requieren un esfuerzo económico y trabajo significativos.	- Compromiso de datos financieros del usuario. - Pérdida de confidencialidad de un número significativo de datos personales por afectado. - Pérdida de confidencialidad de datos sensibles identificables. - Suplantación de identidad. - Degradación de la propiedad. - Pérdida de empleo. - Perjuicio social potencial serio (discriminación, afección física o psicológica).
Violación de privacidad	Critico	El impacto sobre las personas afectadas es crítico. Los posibles inconvenientes son muy difícilmente subsanables o irremediables.	- Riesgo financiero como grandes deudas. - Pérdida de confidencialidad de un número elevado de datos personales por afectado. - Suplantación de identidad con credenciales oficiales (certificados DNI-e, etc.…). - Incapacidad para trabajar. - Perjuicio social potencial permanente (discriminación, afección física o psicológica).

Editor: Secretaria General / UPV · D.L.: V-5092-2006 · ISSN: 1887-2298 · www.upv.es/secgen