PROTOCOLO DE NOTIFICACIÓN DE BRECHAS DE SEGURIDAD DE DATOS PERSONALES DE LA UNIVERSITAT DE VALÈNCIA

ÍNDICE

Primero. Objeto y ámbito de aplicación

1.El procedimiento recogido en el presente Protocolo pretende dar cumplimiento al Reglamento General de Protección de Datos de la Unión (a partir de ahora RGPD) y la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de Derechos Digitales (LOPDGDD) en materia de detección y notificación de violaciones o brechas de seguridad que puedan afectar a la seguridad de datos de carácter personal incorporados a tratamientos que sean responsabilidad de la Universitat de València, independientemente del formato o soporte en el que estén almacenados u organizados.

2. Asimismo tiene por objeto dar cumplimiento a las obligaciones relativas a la gestión, respuesta y documentación-registro a nivel interno de incidentes de seguridad. Una vez detectada la brecha de seguridad, en función de su naturaleza y alcance, la Universitat de València dispone de un plazo de 72 horas para informar a la Autoridad de Control competente, valorar su posible notificación a la Agencia Española de Protección de Datos y, en su caso, cuando la brecha de seguridad pueda entrañar un alto riesgo para los derechos y libertades de los titulares de los datos, su comunicación a los afectados.

3**.** El presente procedimiento será de aplicación a cualquier usuario de los sistemas de información de la Universitat de València implicado en el tratamiento de datos de carácter personal, ya sea miembro del personal docente investigador (PDI), personal investigador en formación (PIF), personal de administración y servicios (PAS) estudiantes o personas externas que se conectan e interactúan con tales sistemas de información vía web institucional o por acceso físico a la documentación.

Segundo. Brechas de seguridad. Concepto e identificación

1.Una brecha es una exposición innecesaria de información o datos de carácter personal que puede conducir a su visualización, captura o manipulación por terceros no autorizados.

El RGPD define, de un modo amplio, las “violaciones de seguridad de los datos personales” como: “todas aquellas violaciones de la 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 autorizados a dichos datos.” Suelen clasificarse en las siguientes categorías:

- Brecha de confidencialidad: acceso a la información por quien no está autorizado o tiene un propósito ilegítimo para acceder a ella.
- Brecha de integridad: cuando la alteración de la información original y la sustitución de datos puede ser perjudicial para el individuo o ilícita.
- Brecha de disponibilidad: impide el acceso a los datos originales cuando es necesario. Puede ser temporal (los datos son recuperables, pero tomará un periodo de tiempo y esto puede ser perjudicial para el individuo), o permanente (los datos no pueden recuperarse).

La Unviersitat de València ha informado y lo hace ahora de las medidas de seguridad que se tienen que adoptar a título individual.

https://www.uv.es/ensuv/es/uvstic-seguridad-tecnologias-informacion-comunicaciones.html

Obviamente, ese tipo de brechas de seguridad individuales tienen que ser informadas al DPD y gestionadas si afectan a datos de la UV, si bien el protocolo se aplica también a todos los ficheros y tratamientos de datos institucionales de la UV.

2.Identificación. Los casos más comunes de posible violación de datos personales son:

- **Acceso a datos no autorizados:**
  - Encargo del tratamiento sin el contrato correspondiente.
  - Acceso indiscriminado a impresoras, fotocopiadoras, etc.
  - Acceso a información confidencial no autorizada: nóminas, currículums, embargos, videovigilancia, etc.
  - Acceso no autorizado a los sistemas informáticos**.**
- **Comunicación no autorizada de datos:**
  - Transmisión ilícita de datos a un destinatario. Error en la dirección de correo.
  - Vulneración del secreto profesional.
  - Publicación de imágenes sin autorización del interesado.
  - Envío de correos electrónicos masivos sin ocultar los destinatarios (copia oculta).
  - Transferencia internacional de datos sin estar sujeta a una decisión de adecuación de la UE o garantías adecuadas de protección de datos.
- **Alteración de datos:**
  - Modificación de datos malintencionada.

- Falsificación de datos.
- Recuperación ineficaz de copias de respaldo.

• Pérdida deinformación:

- Extravío u olvido de soportes (portátil, “pendrive” o disco externo)
- Robo o sustracción de información (portátil, “pendrive” o disco externo)
- Desinstalación de aplicaciones informáticas.
- Por causas del transporte.
- Reorganización de la empresa

• Destrucción de datos:

- No usar destructora de papel o de soportes digitales.
- Incendio, inundación u otras causas ajenas a la empresa.

• En cualquiera de los casos mencionados anteriormente, se pueden producir violaciones de datos por la ausencia de medidas de seguridad:

- Antivirus, antispam, antimalware, antiransomware, firewall, cifrado, “seudonimización”, etc.
- Identificación y autentificación para acceder a los sistemas informáticos.
- Mecanismos de seguridad para acceder al mobiliario o a departamentos con datos personales.
- Disposición de datos a la vista de personas no autorizadas (recepción, monitores, mesas, etc.).

Tercero. Plan de actuación.

1. Detectada e identificada una brecha de seguridad por cualquier usuario de los sistemas de información de la Universitat de València es necesario comunicarlo internamente a efectos de su análisis, clasificación, elaboración de un plan de respuesta con el diseño de las medidas a adoptar para contener, reducir o eliminar posibles daños y, en su el caso inicio del proceso de notificación. No hacerlo sería una infracción grave o leve conforme a la LOPDGDD.

2. A tal efecto, ante cualquier detección de exposición de datos personales bien sean en lugares que incluyan soportes físicos o informáticos, el usuario deberá cumplimentar el formulario del Anexo II, dando el mayor número de detalles necesarios para su análisis y valoración, y enviarlo, mediante correo electrónico, a la Oficina de Protección de Datos de la Universitat de València (lopd@uv.es), sin perjuicio de que, por determinadas circunstancias o por motivos de urgencia, se pueda comunicar telefónicamente al número 661854502 (Delegado de Protección de Datos de la Universitat de València y sus Fundaciones).

3. El Delegado de Protección de Datos, analizará la comunicación para determinar si se está ante una brecha de seguridad relacionada con la protección de datos de carácter personal.

4. En caso de que lo sea, el Delegado de Protección de Datos, con la ayuda del Servicio de Informática, determinarán las medidas correctoras a aplicar y los controles a implementar, comunicándolas a los responsables internos de los tratamientos afectados.

5. El Delegado de Protección de Datos recabará los datos necesarios para, en su caso, comunicarlo a la Agencia de Protección de Datos en el plazo máximo de 72 horas desde su detección y, si procede, a los interesados afectados.

Cuarto. Inscripción de incidentes en el Registro de Brechas de Seguridad de Datos Personales de la Universitat de València

1.Ante cualquier incidente, la Delegación de Protección de Datos abrirá expediente de seguridad de la información en la aplicación creada para gestionar estos incidentes anotándolo como "exposición de información", asimismo dará de alta el expediente en el Registro de Brechas de Seguridad de Datos Personales.

2.El Registro de Brechas de Seguridad de Datos Personales, custodiado por la Delegación de Protección de Datos, contará con la siguiente información respecto de cada incidente de seguridad de datos de carácter personal:

A. Tipo de Notificación (N.º registro, fecha y tipo).

B. Datos del Delegado de Protección de Datos.

C. Datos del Responsable del Tratamiento.

D. Datos del Encargado del Tratamiento (si lo hubiese).

E. Información temporal de la brecha (fecha de detección, medios de detección, justificación de notificación tardía, fecha de inicio de la brecha, estado de resolución).

F. Sobre la brecha:

a. Resumen del incidente.

b. Tipología (confidencialidad, integridad o disponibilidad).

c. Medio por el que se materializó la brecha.

d. Contexto.

e. Medidas preventivas aplicadas antes de la brecha.

G. Sobre los datos afectados:

a. Categoría de los datos.

b. Categorías especiales de datos.

c. Número aproximado de registros de datos afectados.

H. Sobre los sujetos afectados (perfil y número de personas afectadas).

I. Posibles consecuencias:

a. En brecha de confidencialidad.

b. En brecha de integridad.

c. En brecha de disponibilidad.

d. Naturaleza del impacto potencial sobre los sujetos.

e. Severidad de las consecuencias para los individuos.

f. Medidas tomadas para solucionar la brecha y minimizar el impacto con los afectados.

J. Comunicación a los interesados (si se comunica: fecha, número de sujetos informados, medio utilizado, justificación para no informar).

K. Implicaciones Transfronterizas.

L. Datos relativos a incidencia interna (número, fecha, denunciante)

2. En todo caso, la violación o brecha de seguridad quedará reflejada en los pertinentes Registros de Actividades de Tratamiento adicionales y complementarios que se lleve de cada fichero o tratamiento**.**

Quinto. Organización de la gestión y comunicación de Brechas de Seguridad de Datos Personales

- Responsable de la Información: Delegado de Protección de Datos.

- Responsable del Área de Seguridad Informática de la UV y SIUV: análisis y en su caso comunicación de la brecha, así como apertura, si se cree conveniente, de expediente con el CCN (Centro Criptológico Nacional).

ANEXO I

Marco legal

Europeo:

- 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) (artículos 33 y 34).

Nacional

- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (art. 73).

- Real Decreto 3/2010, de 8 de enero (modificado por Real Decreto 951/2015), por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.

Sectorial

- Política de Seguridad de la Información de la Universitat de València aprobada por Junta de Gobierno de la Universitat de València.

- Reglamento de Seguridad de la Información de la Universitat de Valéncia aprobada por Junta de Gobierno de la Universitat de València.

ANEXO II

FORMULARIO PARA NOTIFICACIÓN DE BRECHAS DE SEGURIDAD (para enviar a lopd@uv.es)

Denunciante o notificante. -

DNI/NIE/PASAPORTE:	**Nombre y apellidos:**
Teléfono de contacto:	**Email:**
Unidad/Servicio/Dpto. al que está adscrito en la UV:	

Información temporal de la brecha. -

Fecha de detección de la brecha:

Medios o modo de detección de la brecha:

Resumen del incidente:

Número aproximado de posibles personas afectadas:

Otros detalles y circunstancias:

Valencia a___de_____de 20_____

Fdo:

ANEXO III

Registro de Actividades de tratamento sobre brechas de seguridad

INFORMACIÓN BÁSICA SOBRE PROTECCIÓN DE SUS DATOS PERSONALES APORTADOS	
Responsable:	UNIVERSITAT DE VALÈNCIA
Legitimación:	El tratamiento es necesario para el cumplimiento de una obligación legal aplicable al responsable del tratamiento (art. 6.1.c Reglamento general de Protección de Datos).
Finalidad:	Gestionar el trámite de detección, control y respuesta de brechas de seguridad en la Universitat de València, procediendo, en su caso, a su notificación a la Autoridad de Control y a los interesados.
Destinatarios:	Delegación de Protección de Datos y Servei d'Informàtica de la Universitat de València
Derechos:	Tiene derecho a solicitar el acceso, oposición, rectificación, supresión o limitación del tratamiento de sus datos, tal y como se explica en la información adicional.
Información adicional:	Puede consultar la información adicional y detallada sobre protección de datos en el siguiente enlace: https://www.uv.es/uvweb/universitat/ca/universitat/delegacio-proteccio-dades-/delegacio-1286042855523.html

Asimismo, en el modelo de Registro de Actividades de Tratamiento específico y ampliado de cada fichero se deberán registrar las brechas de seguridad que afecten a cada concreto fichero.