JESUS MANUEL MARTÍNEZ CASTILLO, Secretario de la Comisión de Seguridad de la Información de la Universidad de Murcia, constituida según la Política de Seguridad de la Información que fue aprobada en Consejo de Gobierno de 2 de marzo de 2012, modificada en Consejo de Gobierno de 16 de noviembre de 2018

CERTIFICO:

Que en la sesión de la Comisión de Seguridad de la Información celebrada el día 16 de diciembre de 2020, estando incluidos en el orden del día, se aprobaron los siguientes documentos:

Notificación de brecha de seguridad

Realización Evaluación de Impacto

que corresponden al Anexo de esta certificación.

Jesús M. Martínez Castillo

Secretario de la Comisión de Seguridad de la Información

ANEXO

Notificación brecha de seguridad

Según establece el artículo 33 GDPR, en caso de violación de la seguridad de los datos personales el responsable del tratamiento habrá de notificarla a la autoridad de control sin dilación indebida y en un plazo máximo de 72 horas de haber tenido constancia de la misma, a menos que sea improbable que dicha violación de la seguridad constituya un riesgo para los derechos y las libertades de las personas físicas. Asimismo, el artículo 34 GDPR establece que cuando sea probable que la violación de la seguridad de los datos personales entrañe un alto riesgo para los derechos y libertades de las personas físicas, el responsable del tratamiento la comunicará al interesado sin dilación indebida.

En virtud de lo dispuesto en el artículo 73.1.r) y s) de la Ley Orgánica 3/2018, el incumplimiento de estas obligaciones se considera una infracción grave.

En consecuencia, la Universidad de Murcia en tanto que responsable de tratamientos de datos de carácter personal tiene que determinar el órgano competente para cumplir esta obligación y, asimismo, determinar el procedimiento que ha de seguirse para adoptar esta decisión. Normalmente el conocimiento de este tipo de incidencias se producirá por parte del Vicerrectorado competente y, en concreto, desde ATICA; o, en su caso, a través de incidencias comunicadas al Delegado de Protección de Datos.

Aunque podría pensarse que la Comisión de Seguridad es el órgano más adecuado para adoptar las referidas decisiones, lo cierto es que al tratarse de un órgano colegiado su funcionamiento requiere de la convocatoria previa de la sesión, lo que supone una dificultad relevante dado el exiguo plazo disponible. En consecuencia, dado que la Secretaría General es el órgano competente, según la **Política de Seguridad de la Información de la Universidad de Murcia**, ya que tiene asignada la función de Responsable de la Información, y que la Comisión de Seguridad tiene entre sus funciones la relativa al seguimiento de las decisiones adoptadas por aquel, se propone:

1. Que las decisiones relativas a las obligaciones de los artículos 33 y 34 RGPD se adopten por la Secretaría General de la Universidad de Murcia, previa consulta con el Responsable de los Servicios y el Delegado de Protección de Datos, salvo que la decisión se hubiese adoptado a propuesta suya.
2. Que la notificación a la Agencia Española de Protección de Datos se realice por la Secretaria General.
3. En el caso de las comunicaciones a las personas interesadas, que la comunicación se realizará sin dilación y, en todo caso, en el plazo máximo de cinco días hábiles por el Vicerrectorado competente en función del servicio afectado, salvo que el mismo sea competencia de la Secretaría General. A tal efecto deberá utilizarse un sistema de comunicación que deje constancia de las comunicaciones realizadas, de las que habrá de informarse al Delegado de Protección de Datos en el plazo de diez días.
4. Que en cada una de las sesiones de la Comisión de Seguridad posteriores a la constatación de algún supuesto de los previstos en los artículos 33 y 34 RGPD se informe adecuadamente a dicho órgano, tanto si se ha decido notificar las incidencias a la autoridad de control y las personas afectadas como, en su caso, si no se ha considerado necesario proceder a ello. En este último caso, por parte de la Secretaría General se habrá de presentar un informe explicando las razones por las cuales no se han realizado la correspondiente notificación, que será incorporado como anexo al acta de la sesión.

Realización Evaluación de Impacto

Según el artículo 35 RGPD, cuando sea probable que un tipo de tratamiento entrañe un alto riesgo para los derechos y libertades de las personas físicas, el responsable del tratamiento realizará, antes del tratamiento, una evaluación del impacto de las operaciones de tratamiento en la protección de datos personales. Asimismo, el artículo 28 de la Ley Orgánica 3/2018 señala que es obligación del responsable del tratamiento valorar si procede llevar a cabo una evaluación de impacto en la protección de datos (EIPD).

En consecuencia, cuando se dieran las circunstancias referidas, por parte de la Universidad de Murcia como responsable de tratamientos de datos de carácter personal y con anterioridad al inicio del tratamiento, debería llevarse a cabo un análisis en los términos establecidos en dicho precepto y teniendo en cuenta las indicaciones formuladas por la Agencia Española de Protección de Datos.

Según la **Política de Seguridad de la Información de la Universidad de Murcia** corresponde a la Comisión de Seguridad aprobar los procedimientos de seguridad, de manera que debiera ser este órgano colegiado quien establezca las condiciones de cumplimiento de la referida obligación. Al tratarse de un órgano de composición múltiple donde participan los diversos responsables institucionales de la Universidad de Murcia, se considera la instancia más idónea para adoptar las decisiones en esta materia.

En consecuencia, se propone:

1. Que la decisión de llevar a cabo una Evaluación de Impacto en materia de Protección de Datos (EIPD) corresponde a la Comisión de Seguridad de la Información, a propuesta de la Secretaría General, del Delegado de Protección de Datos o del Responsable de los Servicios.
2. Que dicha decisión se pronuncie en todo caso acerca de la necesidad de recabar la opinión de los interesados en los términos del artículo 35.9 RGPD. A tal efecto se pondrá en marcha un procedimiento de información pública con una duración mínima de quince días hábiles, anunciado con suficiente antelación a través de las listas oficiales de correo-e de la UMU que correspondan, en el que existirá la posibilidad de participar por medios telemáticos sin necesidad de identificación por parte de quien realice las alegaciones. La decisión de no llevar a cabo este trámite deberá ser motivada.
3. La elaboración del correspondiente análisis previo se realizará por la Secretaría General como Responsable de la Información. En el documento correspondiente se incorporará un anexo con la transcripción literal de todas las aportaciones obtenidas durante la fase de información pública a que se refiere el apartado anterior.
4. En todo caso, será preceptivo el informe del Responsable de los Servicios y del Delegado de Protección de Datos sobre el análisis previo realizado por la Secretaría General.
5. La aprobación definitiva de la EIPD corresponderá a la Comisión de Seguridad, cuyos miembros habrán de tener acceso a la totalidad de la documentación referida en los apartados anteriores.