SEGURIDAD DE LA INFORMACIÓN EN LA INSTITUCIÓN UNIVERSITARIA

INFORMATION SECURITY AT THE UNIVERSITY

Autor:

Ricard Martínez Martínez, Cátedra de privacidad y Transformación Digital Microsoft-Universitat de València ricard.martinez@uv.es ORCID 0000-0003-3297-6385

Resumen:

En este trabajo se analizan los requerimientos de seguridad que derivan de la aplicación del Reglamento General de Protección de Datos. Además de una sucinta exposición se identifican los factores de riesgo que a juicio del autor afectan a la institución universitaria. En este sentido a la complejidad estructural y funcional se une una cultura interna que dificulta significativamente el despliegue de modelos de cumplimiento y gobernanza.

Abstract:

This paper analyses the security requirements deriving from the application of the General Data Protection Regulation. In addition to a brief description, it identifies the security risk factors that, in the author's opinion, concern the university institution. In this regard, in addition to the structural and functional complexity, there is an internal culture that significantly hinders the deployment of compliance and governance models.

Palabras clave:

Privacidad; Seguridad; Protección de datos

Keywords:

Privacy; Security; Data Protection

1. LA SEGURIDAD: UN OBJETIVO ESENCIAL DEL REGLAMENTO GENERAL DE PROTECCIÓN DE DATOS

El Reglamento General de Protección de Datos (RGPD) define una aproximación a la seguridad, y por ende a la ciberseguridad, que implica ineludiblemente un diseño centrado en el análisis de riesgos y en su caso, en la evaluación de impacto en la protección de datos. La idea esencial, el mensaje claro que sin duda lanza el Reglamento es que sin seguridad no puede existir una garantía adecuada de la privacidad. Por ello, el RGPD sitúa la seguridad entre los principios del artículo 5 como uno de los principios nucleares en torno a los cuales gira la garantía del derecho a la protección de datos y el principio de responsabilidad proactiva.

Además, supera el tradicional marco de valores que integra la confidencialidad, la integridad, y la disponibilidad, para incluir el concepto de resiliencia. Esto tiene un significado crucial e implica que las organizaciones que tratan datos, y los propios tratamientos, deben ser capaces de sobreponerse, incluso a eventos de naturaleza catastrófica. Por tanto, la resiliencia incorpora un valor añadido desde el punto de vista del esfuerzo que una organización debe realizar en materia de seguridad, confiriendo a la misma la solidez la capacidad de sobreponerse a los más graves incidentes.

Complemento indispensable de la estrategia reglamentaria en esta materia, lo constituyen las notificaciones de violaciones de seguridad, que han ocupado de manera particularmente intensa a la División de Innovación Tecnológica de la Agencia Española de Protección de Datos (AEPD). En este sentido, tal y como refleja la Memoria del año 2020, la notificación de violaciones de seguridad y su evaluación es entendida como verificación de la diligencia, como remedio y propuesta de actuación, antes que como procedimiento sancionador. Ello implica una aproximación adecuada y ordenada a la consecución de lo que sin duda son objetivos de la normativa en la materia, esto es, proporcionar confianza, robustez y una metodología que empodere a las organizaciones para ser capaces de hacer frente a los retos que la seguridad de la información les plantea.

Sin embargo, queda mucho camino por recorrer. Debe subrayarse, que la ciberseguridad está alcanzando una dimensión particularmente estratégica en la medida en la que se trata de un fenómeno complejo en el cual los agentes generadores de ataques se multiplican de modo significativo. Así, a la panoplia de ataques tradicionales debemos sumar la consolidación en el último decenio de bandas organizadas que hacen de la ciberdelincuencia su objeto de negocio. En el último periodo las amenazas vinculadas a las estrategias de ciberguerra de determinados estados ocupan un lugar privilegiado.

En este sentido, el diagnostico de ENISA es contundente. En primer lugar, de abril de 2020 a julio de 2021 las 9 principales amenazas identificadas son:

1. *Ransomware*;
2. *Malware*;
3. *Criptojacking*;
4. Amenazas relacionadas con el correo electrónico;
5. Amenazas contra los datos;
6. Amenazas contra la disponibilidad y la integridad;
7. Desinformación - desinformación;
8. Amenazas no maliciosas;
9. Ataques a la cadena de suministro

En cuanto a las tendencias, durante el periodo del informe se destacan las siguientes:

> "El ransomware ha sido evaluado como la principal amenaza para 2020-2021.
>
> Las organizaciones gubernamentales han intensificado su juego tanto a nivel nacional como internacional.
>
> Los ciberdelincuentes están cada vez más motivados por la monetización de sus actividades, por ejemplo, el ransomware. La criptomoneda sigue siendo el método de pago más común para los actores de amenazas.
>
> El descenso del malware que se observó en 2020 continúa durante 2021.
>
> El volumen de infecciones por criptojacking alcanzó un récord en el primer trimestre de 2021, en comparación con los últimos años. La ganancia financiera asociada al criptojacking incentivó a los actores de amenazas a llevar a cabo estos ataques.
>
> COVID-19 sigue siendo el señuelo dominante en las campañas de ataques por correo electrónico.
>
> Hubo un aumento de las violaciones de datos relacionadas con el sector sanitario.
>
> Las campañas tradicionales de DDoS (Denegación de Servicio Distribuida) en 2021 son más específicas, más persistentes y cada vez más multivectoriales. El IoT (Internet de las cosas) junto con las redes móviles está dando lugar a una nueva ola de ataques DDoS.

> En 2020 y 2021, observamos un repunte de los incidentes no maliciosos, ya que la pandemia del COVID-19 se convirtió en un multiplicador de los errores humanos y de las desconfiguraciones de los sistemas, hasta el punto de que la mayoría de las infracciones en 2020 fueron causadas por errores".

Por su parte en su informe de 2021 el CCN-CERT rubrica en su resumen ejecutivo "Récord de incidentes de seguridad, digitalización forzosa e incertidumbre: las claves de 2020". En este sentido, el informe destaca el papel de los llamados "Actores Estado" respecto de los que señala:

> "En los últimos años, los Estados han sido uno de los principales actores de la amenaza, y han evolucionado su actividad para alinearse con los objetivos políticos de los países donde operan. De hecho, implicando un cambio de tendencia, en el último año el 90% de los objetivos han sido contra organismos públicos, ONG y entidades de políticas sociales o asuntos internacionales.
>
> Por sectores, han sido objetivos prioritarios de los actores Estado o grupos patrocinados por estos aquellos vinculados a los actuales conflictos y problemáticas globales, como la crisis sanitaria o el escenario multipolar de política internacional, entre otros. Estos han sido los principales sectores de interés:
>
> - Gubernamental
> - Defensa
> - Industria armamentística
> - Salud e industria farmacéutica
> - Centros de investigación
> - Tecnologías de la información y las comunicaciones
> - Energía
> - Telecomunicaciones
> - Inversión financiera
> - Comercio internacional"

En este sentido, asistimos, a una manifiesta desconfianza de la Unión Europea en relación con los ataques que se vienen recibiendo desde otros países. Se trata de intervenciones de las unidades de ciberguerra formales o informales asociadas a potencias que atacan recursos e infraestructuras críticas, y que han llevado a algún gobierno a considerar prescindir de metodologías de voto electrónico con la finalidad de asegurar la certeza y transparencia en sus procesos electorales.

2. SEGURIDAD EN LAS INSTITUCIONES UNIVERSITARIAS

2.1 Marco general

En los procesos de formación vinculados a la garantía de la seguridad de los sistemas de información se recurre frecuentemente a un conjunto de frases tópicas particularmente contundentes. Uno ya se ha señalado: sin seguridad no existe la privacidad. En segundo lugar, se subraya que el eslabón más débil en el ámbito de la seguridad son las personas. Finalmente, cuando se trata de comprometer al conjunto de la organización, y en particular a sus órganos directivos no es infrecuente hacer alusión a alguna catástrofe significativa en el pasado inmediato. Aquí, constituye un clásico la alusión a los atentados de las Torres Gemelas, para señalar que tras el 11S existieron dos tipos de empresas: aquellas que pudieron operar en las 24 horas siguientes, y las que desaparecieron. Detrás de todos y cada uno de estos tópicos existe una realidad subyacente que permite identificar los elementos cruciales a los que nos enfrentamos para el despliegue de la seguridad en los sistemas de información universitarios.

En primer lugar, debemos abordar el conjunto de requerimientos que derivan del RGPD y del marco específico aplicable a la seguridad de las instituciones universitarias en España. En segundo lugar, debemos identificar o debemos referirnos a la cultura de la organización a la cultura de la seguridad en nuestras organizaciones, para finalmente referirnos a los valores que una adecuada política de seguridad puede aportar a la institución universitaria.

De otra parte, debe señalarse que el RGPD es particularmente parco a la hora de identificar las medidas de seguridad aplicables a los sistemas de información. En este sentido, existen únicamente referencias expresas a medidas concretas cuando el se refiere a la seudominimización y al cifrado. Medidas que considera particularmente adecuadas en el artículo 32 RGPD, y que tiene en consideración cuando se trata de evaluar el impacto de un evento dañoso al efecto de considerar la eventual notificación de una violación de seguridad.

Por otra parte, el RGPD define la seguridad como un objetivo alcanzable como una obligación de medios, no de resultado que debe suponer un balance adecuado entre el análisis de riesgos realizado por la organización y por otra parte la consideración de los medios que razonablemente desplegados deberían poder conseguir el objetivo de proporcionar unas garantías adecuadas:

> "(83) A fin de mantener la seguridad y evitar que el tratamiento infrinja lo dispuesto en el presente Reglamento, el responsable o el encargado deben evaluar los riesgos inherentes al tratamiento y aplicar medidas para mitigarlos, como el cifrado. Estas medidas deben garantizar un nivel de seguridad adecuado, incluida la confidencialidad, teniendo en cuenta el estado de la técnica y el coste de su aplicación con respecto a los riesgos y la naturaleza de los datos personales que deban protegerse. Al evaluar el riesgo en relación con la seguridad de los datos, se deben tener en cuenta los riesgos que se derivan del tratamiento de los datos personales, como 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, susceptibles en particular de ocasionar daños y perjuicios físicos, materiales o inmateriales"

Desde otro punto de vista, el Reglamento remite a la estandarización de la seguridad. Así, los artículos 40 y 42, se refieren sucesivamente a los códigos de conducta y a los esquemas de certificación. Estos instrumentos permiten en seguridad definir un conjunto de metodologías de análisis de riesgos, de implementación de las medidas de seguridad concretas, y de gestión de las eventuales violaciones o brechas de seguridad. Se trata de procesos formalizados, verificables y certificables.

Por otra parte, la definición de las obligaciones y condiciones concretas de seguridad puede formar parte del margen de apreciación que el RGPD conceden a los Estados. De ahí que, en la disposición adicional primera sobre medidas de seguridad en el ámbito del sector público de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD) ha ampliado el alcance del llamado Esquema Nacional de Seguridad (ENS) como estándar aplicable al conjunto de los entes que define el artículo 77.1 LOPDGDD. Ello implica, que la inmensa mayoría de las universidades deberían aplicar dicho estándar, no afectando al menos en principio

a las universidades de titularidad privada. En función de la personalidad jurídica de cada institución universitaria, podemos abordar tres escenarios:

- Universidades que vienen obligadas a aplicar el Esquema Nacional de Seguridad incluido su entorno fundacional y corporativo.
- Universidades que en virtud de las habilitaciones que les concede el RGPD y tras el oportuno análisis de riesgos y o evaluación de impacto definen su propio estándar de medidas.
- Universidades públicas o privadas que optan por un estándar certificable distinto del ENS. A condición, en el caso de las primeras de que se pueda asimilar a este último.

En nuestra opinión, el ENS posee la capacidad de constituir un referente razonable de seguridad para el conjunto de la universidad española por diversas razones. Se trata de un estándar que cuenta con una panoplia de herramientas para su despliegue. En efecto, el sector público cuenta con recursos significativos para definir e implementar sus políticas de seguridad:

- La metodología MAGERIT por la Administración General del Estado.
- El despliegue normativo del Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica (ENS).
- Las guías y herramientas proporcionadas por el Centro Criptológico Nacional.

Este conjunto integra uno de los modelos mejor acabados en cuanto a estándares y certificaciones de seguridad. Sin embargo, el grado de implantación por sus principales destinatarios, esto es, por las Administraciones Públicas resulta relativamente bajo y manifiestamente insatisfactorio. En este sentido se han registrado certificaciones de:

- 9 entidades en la Administración General del Estado.
- 27 en las Comunidades Autónomas.
- 10 entidades locales.

- 6 Universidades.
- 34 entidades pertenecientes al Sector Público Institucional.
- 393 empresas potencialmente proveedoras de servicios.

Estas cifras no se refieren en absoluto a una certificación integral, en la mayor parte de los casos afectan a sistemas o subsistemas de información y/o servicios determinados.

2.2 La especificidad universitaria

Reflexionar sobre la especificidad universitaria obliga integrar elementos de carácter objetivo junto con una ineludible alusión a la experiencia subjetiva de quien redacta estas líneas.

Desde un punto objetivo, si algo caracteriza a la institución universitaria es su carácter complejo, y el hecho de tratarse de una institución que, tanto en el sector público, como en el privado, despliega múltiples funciones que comportan paralelos tratamientos de datos de carácter personal. En este sentido, el marco básico de acción de la institución universitaria viene definido por el artículo 1 de la Ley Orgánica 6/2001, de 21 de diciembre, de Universidades (LOU) en los siguientes términos:

> **Artículo 1. Funciones de la Universidad.**
> 1. La Universidad realiza el servicio público de la educación superior mediante la investigación, la docencia y el estudio.
> 2. Son funciones de la Universidad al servicio de la sociedad:
> a) La creación, desarrollo, transmisión y crítica de la ciencia, de la técnica y de la cultura.
> b) La preparación para el ejercicio de actividades profesionales que exijan la aplicación de conocimientos y métodos científicos y para la creación artística.
> c) La difusión, la valorización y la transferencia del conocimiento al servicio de la cultura, de la calidad de la vida, y del desarrollo económico.
> d) La difusión del conocimiento y la cultura a través de la extensión universitaria y la formación a lo largo de toda la vida.

Adicionalmente, puede rastrearse en el conjunto del articulado de la LOU obligaciones/habilitaciones adicionales que relacionadas con la calidad en la docencia, o la prestación de servicios específicos a la comunidad universitaria implican tratamientos de datos particularmente sensibles. Por otra parte, las obligaciones que la legislación laboral impone a su vez a la universidad comportan de nuevo tratamientos de datos

sujetos a especiales riesgos. En este sentido, y en una enumeración que no pretende ser en absoluto exhaustiva, cabe referirse a un conjunto de tratamientos que afectan a nuestra gestión ordinaria y que obligan a un adecuado despliegue de la seguridad:

- Gestión de recursos humanos y prevención de riesgos laborales.
- Videovigilancia y seguridad de los campus.
- Gestión académica, incluidas las políticas de integración y prestación de servicios a personas con discapacidad.
- Cuestiones relacionadas con la analítica del desempeño y la calidad en la docencia, la investigación y el aprendizaje.
- Entornos de gestión de altísima complejidad en clínicas universitarias propias vinculadas a las titulaciones de odontología, fisioterapia, podología, psicología, nutrición, etc.
- Centros de innovación e investigación basada en personas marketing y neuromarketing, menores, trastorno del espectro autista, simuladores de realidad virtual… etc.
- Gestión de actividades y eventos de toda naturaleza: académica, investigadora, deportiva, cultural, etc.

Debemos incluir el marco gestión de los sistemas de información vinculados a estas finalidades y de entornos complejos de telecomunicaciones que no sólo conectan los campus a través de las tecnologías más avanzadas, sino que insertan a la institución universitaria en redes de supercomputación de ámbito nacional e internacional.

Un segundo elemento, que no suele considerarse se refiere al rol de la propia institución universitaria como encargado del tratamiento. En este sentido, lo usual es que un entorno corporativo integrado por fundaciones, y en ocasiones por entidades empresariales propias o en participación, soporte sus sistemas de información en los recursos de la universidad dando un lugar a escenarios de complejidad en los que se juega a la vez el papel de responsable, corresponsable o encargado del tratamiento según la tarea que se despliegue.

Capítulo aparte, merece el conjunto de tratamientos que se vinculan al despliegue de la actividad investigadora. Basta con consultar la memoria de investigación de cualquier universidad, o los datos que eventualmente puede proporcionar la FECYT, para apreciar hasta qué punto las universidades se ven inmersas en procesos de investigación vinculadas a entornos de una alta intensidad de requerimientos en lo relativo al cumplimiento del RGPD. En este sentido, el desarrollo de la investigación en el área de salud, la existencia de equipos particularmente relevantes y avanzados en el despliegue de soluciones de analítica de datos e inteligencia artificial, o la significativa capacidad de la institución universitaria para producir innovación en campos como el software, las aplicaciones móviles, o las APIs, demuestran el enorme nivel de exigencia que desde el punto de vista de la garantía de la seguridad en todos estos entornos resulta necesario garantizar.

Sin embargo, y desde el punto de vista de la experiencia subjetiva de quien escribe estas líneas, se constatan significativas carencias desde un punto de vista organizativo que en la práctica acaban por golpear de modo recurrente a nuestras instituciones. Seguramente el último ejemplo conocido, sea el alto grado de litigiosidad que ha generado la implementación de procedimientos de reconocimiento facial puestos en exámenes online denunciados por las personas interesadas, discutidos de modo significativo por la AEPD y susceptibles de generar un altísimo riesgo de incumplimiento normativo desde el punto de vista de la garantía de lo previsto en el artículo 9 RGPD, pero también desde el de la seguridad.

Este caso constituye la anécdota más que la categoría. La realidad para cualquier conocedor de la institución universitaria obliga a alertar sobre el grado en que la independencia y la autonomía de decisión que la libertad de investigación y de cátedra han conferido a ciertas unidades o personas se traslada negativamente a las capacidades para garantizar la seguridad en el tratamiento de la información. El número de sujetos con probada capacidad para originar de modo autónomo, un tratamiento de datos sin una adecuada supervisión constituye por sí mismo un riesgo para la seguridad de la información. En este sentido, no resulta extraño constatar a lo largo de los años un

conjunto de prácticas usuales que, si bien tienden a reducirse, resultan todavía presentes en muchas de nuestras instituciones.

En primer lugar, las facilidades que ofrece la ofimática y en particular los recursos en la nube a disposición de los usuarios privados facilitan el despliegue de decisiones autónomas, no notificadas ni a la autoridad académica, ni a la persona delegada de protección de datos y/o a la responsable de seguridad. Nos referimos, por ejemplo, a la proliferación de pretendidas encuestas anónimas integradas en soluciones privadas sin ningún tipo de contrato con la institución universitaria y mediante el registro de carácter privado del investigador o estudiante que desarrolla la actividad. Exactamente el mismo fenómeno, se produce en decenas de eventos universitarios en los cuales, mediante el simple expediente de copiar y pegar unas políticas de privacidad, se acaba registrando a los asistentes en entornos no autorizados, incumpliendo con las obligaciones que el RGPD impone a responsables del tratamiento y encargados, y sin ninguna verificación de la confiabilidad y la seguridad de la solución escogida.

Otro fenómeno recurrente, consiste en el desarrollo de soluciones informáticas propias, ya sea porque se tiene la capacidad técnica para hacerlo, ya sea por tratarse de un supuesto de contratación menor de bajos requerimientos en su control y al alcance de la competencia y los recursos de la unidad, el centro o departamento. Esta acción autónoma, ha conducido, en más de una ocasión, a grandes brechas de seguridad que han debido ser notificadas tanto a la autoridad de control competente como a las personas interesadas.

No debemos olvidar los procesos vinculados a la investigación. Resulta particularmente preocupante que en muchas ocasiones no se sea capaz de identificar el rol en virtud del cual se tratan datos personales. Nos referimos, a supuestos de personal con plaza vinculada o profesorado asociado que extrae datos de otras organizaciones que utiliza con posterioridad para la docencia o la investigación. En estos casos, no existe ninguna trazabilidad universitaria sobre el uso de los datos excepto la relativa a la exportación del

sistema de información origen de los datos. Se trata de datos que acaban alojados en ordenadores, soportes informáticos e incluso en el aula virtual de la universidad.

En todos y cada uno de los supuestos aquí mencionados, suele darse un patrón común. El usuario, que posee las capacidades tanto para obtener los datos como para desarrollar algún tipo de tratamiento, no se ha ajustado a los protocolos que la institución ha definido para notificarlo o para gestionar desde el punto de vista ético y jurídico la investigación. Únicamente, en aquellos casos en los que resulte necesario el informe favorable de un Comité de ética, existe la posibilidad remota de identificar los riesgos para la seguridad de un tratamiento con anterioridad a su ejecución material.

Podrían extenderse los ejemplos de riesgo en esta materia, pero en nuestra opinión, basta con los señalados para identificar los graves problemas a los que podría enfrentarse una institución universitaria. Estos se resumen esencialmente en dos. El primero, derivaría de tratamientos de datos no comunicados susceptibles de incumplir el conjunto del ordenamiento prácticamente en cascada, y de afectar de modo muy grave a la seguridad de la información. El segundo, deriva del uso de recursos poco confiables, o de la contratación de sujetos o entidades incapaces de garantizar los requerimientos que el artículo 28 RGPD impone a un encargado del tratamiento en materia de seguridad.

2.3 El origen de los riesgos: formación y gobernanza

Como se viene señalando a lo largo de este texto, una gran parte de nuestras afirmaciones responden a criterios ciertamente subjetivos. Es un hecho innegable que a la sombra del Esquema Nacional de Seguridad y del Reglamento de desarrollo de la Ley Orgánica 15/1999 (Real Decreto 1720/2007) las universidades españolas se proveyeron de políticas y de normativas de seguridad. En el periodo 1999-2010 procedieron a un enfoque sistemático de la cuestión, así como a la documentación de las medidas de seguridad adoptadas y a su auditoría regular. Estas políticas se han proyectado de manera eficiente y con resultados en principio positivos en los sistemas de información directamente gestionados por los tradicionalmente denominados servicios de informática, centros de proceso de datos o servicios de tecnologías de la información y las

comunicaciones. No obstante, el bajo índice de sistemas de información certificado con el ENS, así como un entendimiento laxo de las obligaciones derivadas de la Ley Contratos del Sector Público (Ley 9/2017) en las exigencias de seguridad en los procesos de contratación de proveedores de servicios siguen ofreciendo un amplio campo a los esfuerzos de mejora.

No obstante, desde la más pura apreciación subjetiva a la que me vengo refiriendo se perciben dos grandes riesgos, cuya solución debería aportar un incremento significativo de la calidad y la confianza en la gestión de la seguridad por parte de la institución universitaria.

En primer lugar, la formación en protección de datos con carácter obligatorio y para el conjunto de la plantilla sigue siendo una entelequia en la mayor parte de las organizaciones universitarias. Debe señalarse, que en algunos casos se han emprendido procesos de formación que abarcan al conjunto del personal de administración y servicios, proporcionando una pátina cultural imprescindible para la garantía del derecho fundamental a la protección de datos. También constan, esfuerzos puntuales de culturización en materia de seguridad siguiendo los modelos formativos y promocionales propuestos por el INCIBE.

Desgraciadamente, en la mayor parte de los casos, las políticas formativas adolecen de carencias significativas. De un lado suelen afectar exclusivamente a una determinada categoría profesional y en la mayor parte de los casos integran la oferta de formación continuada de carácter de carácter voluntario. Cuando esto es así, la estrategia formativa lejos de mejorar las condiciones de cumplimiento tiende a empeorarlas de manera significativa. Y ello es debido a varias razones. La primera, porque precisamente la naturaleza voluntaria de la misma tiene como consecuencia una penetración asimétrica en los distintos niveles que no se corresponde con un diseño estratégico del cumplimiento en materia de privacidad y seguridad. De hecho, este modo de formar puede ser un semillero de conflicto. No es infrecuente que el personal sin capacidad de decisión se enfrente a situaciones de incumplimiento, para las que ha sido formado, ordenadas por

superiores sin formación alguna. Por otra parte, esta culturización asimétrica y no coordinada estratégicamente con un modelo de *compliance* es fuente de constantes notificaciones y consultas a los delegados de protección de datos saturando sus capacidades de gestión. Así, en ausencia de un diseño global de cumplimiento, se convierte a estos profesionales en apagafuegos o "recolecta-setas", usando una expresión coloquial. Y quienes conocen la jerga entienden perfectamente a qué nos estamos refiriendo.

Un segundo error manifiestamente significativo consiste en no haber sido capaces de segmentar la formación diferenciando claramente al menos tres niveles. Las responsabilidades en protección de datos de las personas que integran los órganos de gobierno o puestos de naturaleza directiva y/o política, no sólo deberían definirse sino también formarse y educarse. En segundo lugar, resulta muy grave cuando se da una carencia de una formación estratégica ordenada a la conformación de cuadros técnicos capaces de trasladar mediante la debida capilaridad las decisiones que en materia de protección de datos y seguridad adopte la institución. El último, y seguramente más grave error consiste en no invertir en la formación del personal docente e investigador. Esta categoría de la mano de la investigación, de la dirección de trabajos finales de grado y master, tesis doctorales, y de la gestión y organización de eventos, son las más proclives a infringir el marco normativo y de seguridad en protección de datos sencillamente por ignorancia.

Y esto acaece en un contexto en el que la mayor parte de las organizaciones se ha limitado a cubrir el expediente nombrando aquellos puestos que conforme al esquema nacional de seguridad y a la legislación sobre protección de datos resultaban de carácter obligado. Cuando no a externalizar los servicios al menor coste posible. Este es un mal común a la mayor parte del sector público español. La seguridad y la privacidad no se dotan de recursos suficientes, ni se impulsan modelos de cumplimiento normativo que integren algún tipo de gobernanza clara y precisa.

El resultado práctico, no es otro que la existencia de profesionales como los delegados de protección de datos y los responsables de seguridad que operan como cuellos de botella en sus organizaciones, puesto que en lugar de aplicar los principios de protección de datos y seguridad desde el diseño y por defecto integrando de modo armónico todo aquello que tiene que ver con la seguridad, se ven condenados a ocuparse de manera permanente en la solución de incidentes que pudieron haberse evitado fácilmente.

3. CONCLUSIONES

El espacio disponible para un artículo de esta naturaleza, y los objetivos perseguidos por el autor han determinado una estrategia de aproximación al problema de carácter sintético y basada en la experiencia. Queda en el tintero una exposición detallada del proceso que debería regir en un modelo gobernado de cumplimiento del Reglamento General de Protección de Datos basado en metodologías de protección de datos desde el diseño y por defecto.

Es evidente, que el proceso que va de la concepción original de un tratamiento de datos personales a su inclusión en el registro de actividades de tratamiento es sin duda el procedimiento óptimo para consolidar un modelo de madurez desde el punto de vista de la seguridad. El diseño inicial, debidamente notificado debe ser soportado y dotado del oportuno acompañamiento y soporte por parte de la organización en términos de gestión, por el responsable de seguridad y por la persona delegada de protección de datos. Y ello debe suceder en un contexto donde el conjunto de la organización disponga de una sólida cultura de protección de datos.

Mientras esto no suceda, mientras no exista una apuesta orgánica clara por parte de la institución universitaria en esta materia, los riesgos para la seguridad y para la garantía del derecho fundamental a la protección de datos seguirán siendo uno de los mayores quebraderos de cabeza para las y los delegados y delegadas de protección de datos. Aplicaremos el RGPD, la LOPDGDD y el ENS de modo epidérmico. Y puede que creamos que protegemos datos mientras en la práctica ponemos en riesgo y desprotegemos a las personas.

Por ello, resulta urgente adoptar decisiones estratégicas que impulsen la dimensión de protección de datos del Esquema Nacional de Seguridad, así como las condiciones que garanticen su plena aplicación no sólo por las Administraciones Públicas directamente, sino por los proveedores de servicios que tratan de datos en su condición de encargado del tratamiento y se encuentran vinculados no sólo por el artículo 28 RGPD sino por el particularmente exigente régimen jurídico de la Ley 9/2017, de 8 de noviembre, de Contratos del Sector Público, por la que se transponen al ordenamiento jurídico español las Directivas del Parlamento Europeo y del Consejo 2014/23/UE y 2014/24/UE, de 26 de febrero de 2014.

4. BIBLIOGRAFÍA

- CCN-CERT. *Guías*. Disponible en https://www.ccn-cert.cni.es/guias.html
- CCN-CERT. *Soluciones de seguridad*. Disponible en https://www.ccn-cert.cni.es/soluciones-seguridad.html
- CCN-CERT. *IA-13/21 Ciberamenazas y Tendencias. Edición 2021*. Disponible en https://www.ccn-cert.cni.es/informes/informes-ccn-cert-publicos/6338-ccn-cert-ia-13-21-ciberamenazas-y-tendencias-edicion-2021-1/file.html
- CCN-CERT. *Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información (MAGERIT v3).* Disponible en https://www.ccn-cert.cni.es/en/gestion-de-incidentes/lucia/23-noticias/551-nueva-version-de-magerit.html_
- ENISA *Threat Landscape 2021*. Disponible en https://www.enisa.europa.eu/publications/enisa-threat-landscape-2021
- INCIBE. *Catálogos de formación en ciberseguridad.* Disponible en https://www.incibe.es/catalogos-formacion-ciberseguridad