Universitat Oberta de Catalunya

uoc.edu

Adaptación de una pyme al RGPD

Nombre Estudiante
Miguel Villanueva Hernández
Área del trabajo final: Seguridad de la Información

Nombre Consultor/a Marco Antonio Lozano Merino
Nombre Profesor/a responsable de la asignatura Víctor García Font

4-6-2018

FICHA DEL TRABAJO FINAL

Título del trabajo:	*Adaptación de una pyme al RGPD*
Nombre del autor:	*Miguel Villanueva Hernández*
Nombre del consultor/a:	*Marco Antonio Lozano Merino*
Nombre del PRA:	*Víctor García Font*
Fecha de entrega:	06/2018
Titulación:	*Máster Universitario en Seguridad de las Tecnologías de la Información i de les Comunicaciones (MISTIC)*
Área del Trabajo Final:	*Seguridad de la información*
Idioma del trabajo:	*Español*
Palabras clave	*Protección datos, seguridad, RGPD*

Resumen del Trabajo:

La nueva normativa relativa a la protección de datos personales para ciudadanos y residentes de la UE está empezando a aplicarse a todas las empresas que procesan datos PII o personales, en la UE. Esta memoria, tratará de adaptar una PYME ficticia, para cumplir con este nuevo Reglamento llamado GDPR. Para ello necesitamos definir primero nuestro tipo de PYME, sus características y principalmente el tipo de datos personales que se deben controlar o procesar. Una vez descrita la empresa a adaptar, analizaremos todos los nuevos requisitos que necesitamos aplicar a nuestra PYME, de acuerdo con el Reglamento, para asegurar su completo cumplimiento.

Hemos elegido una empresa que ofrece un servicio con tecnología de vanguardia, que necesita procesar datos personales de clientes, rol de encargado, junto con sus propios datos personales, rol de responsable. Por lo que, hemos diferenciado ambas soluciones de medidas dependiendo de estos roles. Las medidas particulares propuestas para esta PYME irreal, se han elegido teniendo en cuenta siempre las técnicas actuales, más eficientes, en cuanto a la viabilidad técnica, funcional y de implementación, y que cumplan con los requerimientos del RGPD. También hemos agregado otras medidas no obligatorias pero que aportarán ventajas a nuestra pyme. Describiremos todas las medidas, técnicas y organizativas y también intentaremos analizar los posibles impactos que podría sufrir nuestra empresa.

Abstract (in English, 250 words or less):

New regulation regarding personal data protection for EU citizens and residents is just starting to apply to all companies processing PII data in EU. This Master's thesis shall try to adapt an unreal SME (Small Medium Enterprise) for being compliant with this new Regulation called GDPR. For that purpose we need to define first our kind of SME, its characteristics and mainly the type of personal data that need to process or control. Then we will analyse all the new requirements we need to apply to our SME, according the Regulation, to be GDPR fully compliant.

We have chosen a company offering a state of the art technology service, which needs to process customer personal data as Processor role, together with its own personal data as Controller. So we have differentiate both solutions measures depending these roles. The particular measures proposed for this unreal SME, have been chosen taken into account always the most efficient ones, regarding technical, design viability and implementation to accomplish with GPDR requirements. We have also add others non-mandatory measures in order to improve the compliance and taking advantage of them. We will describe all measures, technical and organizational and also try to review the possible impacts that could suffer our company.

Índice

1. Introducción

1.1 Contexto y justificación del Trabajo

Este TFM va a exponer y analizar los nuevos cambios introducidos por la regulación europea referente a la protección de datos personales, **REGLAMENTO (UE) 2016/679**, más conocido como RGPD (Reglamento General de Protección de Datos o en inglés GDPR [1]), que obliga a su cumplimiento o aplicación, en los 28 países miembros de la UE, a partir del 25 de mayo de este año y que no contemplaba las directivas actuales o en menor grado de exigencia, como la Directiva 95/46/CE. Concretamente nos centraremos en el cumplimiento del Reglamento para una pyme ficticia española, relacionada con el campo de la computación en nube privada y la virtualización de un servicio de comunicación como es la voz sobre IP (VoIP).

El interés en aumento, que suponen los datos personales para las empresas, entra cada vez más en conflicto con los derechos fundamentales, recogidos en las leyes actuales sobre la protección de los mismos: Constitución Española (CE) en su artículo 18, apartados 1 y 4, en el Real Decreto 1720/2007, de 21 de diciembre [2], por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999 (LOPD [3]), de 13 de diciembre, sobre la protección de los datos de carácter personal. Éstas ya ofrecían un marco legal, sobre el tratamiento y la intimidad personal en las comunicaciones, que provocó una tendencia mayor, por la privacidad en las telecomunicaciones en nuestro país. Pero que, debido a la gran revolución digital, a nivel mundial, tanto a nivel empresarial como en la vida de las personas, ha llevado a la UE a desarrollar este nuevo Reglamento en el ámbito de la protección de datos, que supera en protección y requerimientos a los ya existentes en la legislación española y la mayoría de estados miembros de la UE. Creando un nuevo marco regulatorio común en la UE, en el ámbito de la protección de datos personales. Es tal la importancia de este reglamento y así lo reconoce el sector empresarial en todo su ámplio espectro, que la empresa que no lo cumpla se quedará literalmente “fuera del mercado”. De ahí la importancia de este nuevo Reglamento, que está en vigor desde su publicación el 27 de Abril del 2016.

Este reglamento afecta a todos los mercados y a todas las empresas que traten con datos de carácter personal, anteriormente ya conocidos como PII, por sus siglas en inglés (Personal Identifiable Information [4]) que ya recogían otros textos legales en países anglosajones.

Para aportar más valor a este trabajo vamos a hacer el estudio sobre una de las tecnologías, que más suscita hoy en día en sus usuarios, el temor a la fuga o pérdida de datos, que son la empresas que ofrecen servicios en ‘nube’ (Cloud Computing en inglés) y en nuestro caso en un tipo concreto de nube privada, basada en códigos abiertos (Open Source), por las ventajas que tienen respecto a los propietarios. Este tipo de empresas y sobretodo los servicios que ofrecen, se están extendiendo exponencialmente, por las ventajas que ofrecen a las empresas que los utilizan, principalmente, ventajas económicas, de

mantenimiento, ubicuidad del servicio, alta disponibilidad, escalabilidad entre otras, que comentaremos a lo largo de este trabajo.

La empresa o pyme sobre la que centraremos este trabajo estará relacionada con servicios de VoIP, pero con el añadido de su virtualización en la nube, que describiremos más extensamente en el capítulo 3 de este trabajo. La demanda de este tipo de servicios virtuales en nube está aumentando en todos los mercados. Este auge, de empresas del sector IT, que ofrecen este tipo de servicios de nube privada para virtualización de aplicativos concretos a empresas, nos ha llevado a escoger una empresa de estas características.

Para la realización de este trabajo nos centraremos principalmente en las nuevas exigencias y requerimientos, algunas ya contempladas en la ley LOPD, relativas al tratamiento y procesado de datos personales, pero nos centraremos en el cumplimiento exclusivo de una PYME ficticia con domicilio fiscal en España, aunque podría extrapolarse a cualquier otro país de la UE. Hay que decir que aunque nos centremos en una PYME, vamos a comentar todos los cambios más importantes que marca el nuevo Reglamento, aunque solo entremos más en detalle en los requerimientos han de cumplir las empresas más numerosas de la UE que son la PYMES, con unas limitaciones que ya comentaremos más adelante, para no extender demasiado el trabajo en puntos concretos que dependen de un tipo de empresa menos numerosas, pero más grandes en tamaño.

Por lo que la importancia de las PYMES, por el volumen de las mismas respecto a las grandes empresas, nos lleva a centrarnos en este TFM más en la casuística del impacto del nuevo Reglamento sobre este tipo de empresas.

1.2 Objetivos del Trabajo

El Objetivo de este TFM será la de obtener una serie de medidas tanto técnicas como organizativas, que ayude a una pequeña o mediana empresa a cumplir con el Reglamento de protección de datos personales. Para ello hemos escogido una pyme concreta que por sus servicios, aporta un interés adicional, al sector del mundo IT y al avance de la digitalización de las empresas.

los principales requerimientos de la nueva normativa europea de protección de datos personales, entrando más en detalle en los requerimientos específicos que afectan a la mayoría de pequeñas y medianas empresas de un país miembro de la UE y concretamente en el tipo de pyme escogida para su análisis, descrita en profundidad en el tercer capítulo del trabajo. Una vez expuestos los requerimientos generales, nos centraremos en el caso práctico de las medidas necesarias, principalmente las de obligado cumplimiento, de nuestra pyme, para posteriormente comentar otras medidas adicionales que creemos relevantes para la adecuación al nuevo Reglamento de protección de datos personales europeo.

Previo análisis de todas las directrices expuestas en el Reglamento, pasaremos a enumerar los principales requerimientos introducidos, que han de cumplir las

empresas que traten con datos personales de ciudadanos o residentes de la UE. para posteriormente, una vez descrita la empresa escogida, tratar de adaptarla al máximo al reglamento, incluso proponiendo medidas adicionales como hemos comentado anteriormente. Analizaremos los datos personales que tiene que tratar según el rol sobre los mismos, como encargado o como responsable, y ver las medidas para ambos. Primero comentaremos el tipo de datos a procesar o tratar como Responsable, y veremos las medidas necesarias, que son más comunes al resto de empresas de este tamaño, que se basan en el de las relaciones y normativas laborales y para después pasar a describir las más específicas a nuestra empresa, como encargado de los datos de sus supuestos clientes, siendo éstas últimas más concretas al sector tecnológico concreto en el que presta sus servicios.

Por lo tanto nuestra empresa ficticia, al igual que la mayoría de empresas, necesitará procesar datos personales, por lo que tendrá que tomar medidas tanto técnicas, de seguridad como organizativas, como responsable de los datos ("data controller") y como encargado de los datos ("data processor"). Diferenciando las medidas necesarias para ambos roles.

Una vez analizados los datos personales que tendrá que procesar y separados por el tipo de implicación sobre los mismos y por categorías veremos acorde al Reglamento, qué medidas son de obligada aplicación y cuáles en nuestro caso particular no lo serían, aunque en algún caso de no obligada aplicación, recomendaremos su cumplimiento por las ventajas y mejoras que podrá aportar a nuestra pyme.

Por lo que el objetivo final será proporcionar todas las medidas necesarias, tanto a nivel de procedimientos u organizativas, como medidas técnicas o de seguridad, acorde al perfil de nuestra empresa, que harán que cumpla el Reglamento y no tenga que enfrentarse a las posibles penalizaciones contempladas en el mismo, según el requerimiento incumplido.

Una parte importante del objetivo del trabajo es escoger un tipo de empresa que está a la vanguardia de los últimos avances tecnológicos en el mundo IT y de los avances de la digitalización empresarial, lo que le aporta un grado más de interés a este TFM. Para ello hemos escogido una empresa que ofrece, uno de los servicios actuales más de mandados por las empresas, como son los servicios virtuales en nube y en nuestro caso particular del tipo IaaS (Infraestructure as a Service).

Con objeto de tener en cuenta la situación específica de las microempresas y las pequeñas y medianas empresas, el presente Reglamento incluye una serie de excepciones en materia del registro de las actividades referente a los datos personales, para organizaciones con menos de 250 empleados. Además, alienta a las instituciones y órganos de la Unión y a los Estados miembros y a sus autoridades de control a tener en cuenta las necesidades específicas de las microempresas y las pequeñas y medianas empresas en la aplicación del presente Reglamento. El concepto de microempresas y pequeñas y medianas empresas debe extraerse del artículo 2.1, del anexo de la Recomendación 2003/361/CE de la Comisión Europea, como veremos en el sub-apartado 3.1.

1.3 Enfoque y método seguido

Hemos enfocado la solución del problema planteado, la adaptación de una pyme al nuevo RGPD, mediante el análisis de un caso práctico, la forma de poder adaptar cualquier pyme, al nuevo Reglamento de protección de datos personales. La serie de medidas en las que se incluyen también las técnicas y de seguridad, hace que tengamos también que tener un enfoque más técnico, para ese tipo de medidas, pero solo planteando la solución técnica sin necesidad de desarrollarla al completo, dado también el carácter ficticio de la empresa, aunque siempre hemos intentado, hacerla lo más real posible, con detalles concretos del servicio que ofrece, dejando la parte más común, como es la exclusivamente relacionada con el ámbito laboral, un poco más abierta y no entrando tanto al detalle. Hemos creído conveniente, que aportaba más las particularidades del cumplimiento como encargado de los datos por el tipo de servicio más innovador y de vanguardia, que los referentes al ámbito exclusivamente laboral, aunque algunos podrían estar en común.

Este enfoque más técnico del cumplimiento lo hemos creído conveniente, igual que el resto de medidas de tipo más documental u organizativas o control, sin llegar a dar una solución detallada, si no explicando las diferentes formas de hacerlo, a modo de guía, por ejemplo en lo relativo a derechos fundamentales o el reporte de la brechas de seguridad, no hemos creído conveniente más que explicar las formas de hacerlo, sin entrar en la implementación técnica detallada que no aporta mucho al proyecto y lo hubiera extendido demasiado, eso sí siempre recalcando la importancia de acometer la medida para que el cumplimiento del RGPD sea posible.

De los 99 artículos y los 173 considerandos del Reglamento, hemos intentado extraer los requerimientos que afectan exclusivamente a las empresas y que nos obligan a cumplir, tanto como responsable como encargado de los datos. Ya que este es un punto que el Reglamento insiste en diferenciar, dependiendo del rol, en su articulado.

Una vez extraídos los principales requerimientos y diferenciados por roles, se ha procedido con la elección de la empresa en la que realizaremos el análisis y el estudio de su adaptación al RGPD. Esta descripción abarca a parte de las características organizativas y la clasificación del tipo de datos personales que tiene que tratar, una descripción técnica del servicio y la estructura para ofrecer este servicio de vanguardia. Comentando las ventajas que supone este tipo de servicio y la importancia de que cumpla con el Reglamento.

A posteriori una vez detalladas las nuevas medidas, las particularizaremos a nuestra empresa, en más detalle. Estas medidas podrían ser perfectamente, casi en su totalidad, en función de los datos que procesen, los de la mayoría de pymes del mismo sector.

Así, la metodología utilizada, para el desarrollo de este trabajo, ha sido principalmente la del análisis profundo del Reglamento y extraer los nuevos

requerimientos, entendiendo los nuevos conceptos introducidos por el Reglamento en temas de privacidad y protección de datos, como los de "seudonimización", "privacidad por diseño", "minimización de los datos" o "responsabilidad proactiva". Para poder obtener las medidas necesarias a implementar en nuestra empresa para el cumplimiento del RGPD.

Una vez enumeradas todas las medidas genéricas, particularizaremos en las de nuestra empresa, diferenciando los dos roles y las agruparemos por la de obligada aplicación y las que siendo no obligatorias, recomendaremos su uso por las ventajas que aportarán a la empresa en estudio. Para las medidas más técnicas, escogeremos, las que por criterios de diseño, impacto en el servicio, económicos o de implementación, se adaptan mejor a éstos. Por ejemplo, de las diferentes técnicas de seudonimización, qué opción nos puede aportar más a la hora de hacer cumplir con todos los criterios descritos anteriormente.

Por lo que las medidas, las desarrollaremos en dos bloques, las que no estarían obligadas a cumplir las pymes y las que el Reglamento les obliga a cumplir, sin particularizar en ningún tipo de sector, de forma más genérica. Para después particularizar las medidas concretas de nuestra empresa ficticia. También añadiremos los puntos que aunque no son de obligado cumplimiento en nuestra empresa, recomendamos que se implementen, cómo pueda ser la elección de un delegado de protección de datos.

1.4 Planificación del Trabajo

La planificación de este proyecto ha venido marcada por los hitos impuestos en la evaluación continua de la asignatura del trabajo de final de máster, marcados por la entrega de tres pruebas de evaluación continua previas a la entrega de esta memoria, en la que se han ido introduciendo y desarrollando, los diferentes capítulos de esta memoria, añadiéndose a posteriori algunos cambios, que hemos creído conveniente para la mejora del producto final.

Comentar también, que no hemos creído conveniente la presentación de un diagrama de Gannt, con éstos hitos, por lo comentado en el párrafo anterior y por los cambios introducidos después de la entrega de las pruebas de evaluación continuas de la asignatura de este trabajo final.

1.5 Breve sumario de productos obtenidos

El producto final de este proyecto es la de desarrollar un grupo de medidas tanto a nivel técnico como organizativo, a modo de guía y dónde se pueden ver las técnicas que se pueden utilizar para cumplir con una serie de requerimientos, extraídos de un texto exclusivamente legal, que técnicamente no aporta soluciones a los problemas planteados, como pueda ser la seudonimización. Digamos que, intentaremos dar una solución técnica a un problema legal planteado por el RGPD, que al final es lo que le interesa a las empresas. Como analizar el posible impacto de éstas medidas técnicas, su viabilidad en la implementación, o la obligatoriedad o no de su despliegue,

también formarán parte de la solución aportada. Para ello necesitamos describir las posibles soluciones, a cada requerimiento. Al final siempre intentaremos dar la solución más adecuada, a nivel técnico y en base al análisis de las particularidades de nuestra empresa, pero que se podrá extrapolar a muchas otras pymes esas medidas. Implícitamente tendremos en cuenta la viabilidad económica de las soluciones, por ejemplo con sistemas de código abierto y de licencia libre.

Estas medidas que aportaremos, se adecuarán a las técnicas de vanguardia que mejor se adecúan al requerimiento y a las necesidades e intereses de nuestra pyme, que remarcamos de nuevo, podrían valer para cualquier pyme del sector privado, en el análisis inicial, como otra más específicas para un tipo de empresa con un perfil más concreto en un sector como es el de la VoIP.

También puede ayudar a marcar pautas o de guía, para poder hacer otros estudios particulares de adaptación, principalmente en pymes y de cualquier otro sector, ya que el análisis y desarrollo como rol de responsable de los datos, se podría extraer, como una guía de medidas, más genérica, para conseguir este deseado cumplimiento del Reglamento.

1.6 Breve descripción de los otros capítulos de la memoria

Esta memoria constará de 5 capítulos, de los cuales este primero tiene un carácter introductorio exclusivamente. A continuación procederemos en el capítulo 2 a hacer referencia a los requerimientos principales descritos en la normativa, que deberán cumplir la mayoría de empresas, agrupándolos en 8 puntos principales sin concretar para qué tipo de empresa aplican, si no que se pueden considerar cómo los requerimientos básicos para poder cumplir y adaptar la mayoría de empresas al Reglamento.

Una vez descritos estos ocho requerimientos, pasaremos a describir en detalle nuestra empresa a estudio, justificando su elección. Analizaremos y clasificaremos el tipo de datos personales, que deberá tratar, como responsable y como encargado y comentaremos las peculiaridades, que nos permitirán su adaptación en el capítulo 4, hacer el estudio y análisis de las medidas a tomar como responsable de los datos. En el capítulo 5, el principal de la memoria, describiremos más en detalle, las medidas y soluciones necesarias, para el cumplimiento, pero como encargado de los datos, separando las medidas de obligado cumplimiento de las no obligadas, obteniendo el paquetes de medidas a nivel técnico y organizativo, que obligaría el RGPD a cumplir para no ser sancionados. En este capítulo también comentaremos las medidas de no obligado cumplimiento pero que sí recomendamos introducir por sus ventajas y mejoras a nuestra pyme, cerrando el capítulo con un apartado que analiza el impacto de las medidas y la forma de implementarlas.

Cerraremos este trabajo con un capítulo de conclusiones dónde resumiremos y expondremos los resultados obtenidos del análisis de los cambios necesarios y recomendados sobre nuestra empresa ficticia.

2. Nuevas medidas del RGPD

En este capítulo, vamos a analizar el texto legal del Reglamento general de protección de datos (RGPD [1]), para intentar recopilar todos los requerimientos necesarios para la mayoría de empresas. Después de este análisis, hemos podido sintetizar en ocho medidas principales, la mayoría de los cambios y políticas incluyendo las de carácter más técnico y las organizativas o de gestión, que debería aplicar la gran mayoría de empresas, tanto de carácter privado, como del sector público, para cumplir con el RGPD.

Destacar, que a lo largo de la memoria, iremos haciendo referencia a los artículos concretos en que nos basamos para realizar cada medida, y así el lector podrá familiarizarse y encontrarlo de forma más cómoda y evitándonos explicar cada vez que hagamos referencia al mismo. Aunque siempre se tendrá que tener a mano el Reglamento.

Para este apartado, también nos hemos apoyado en las guías y URLs de recomendaciones de la CE (Comisión Europea) como su URL sobre privacidad y protección de datos [4] y de la AGPD (Agencia de Protección de datos española) [5].

En los siguientes apartados de este capítulo pasamos a detallar éstas medidas obtenidas del articulado principalmente, aunque siempre apoyándonos cuando ha sido necesario en el considerando del texto legal. Las utilizaremos en el resto del trabajo y más particularmente a la hora del análisis de cumplimiento de nuestro caso práctico.

2.1 Evaluaciones del impacto de protección de datos (EIPD)

Una de las primeras medidas que tendrán que cumplir muchas de las empresas será la de las Evaluaciones de impacto de la protección de datos o EIPD, según sus siglas en inglés, las DPIA, (Data Privacy Impact Assessments). El responsable del tratamiento realizará, antes del tratamiento, una evaluación del impacto de las operaciones de tratamiento en la protección de datos personales. Y acorde al art. 35, la evaluación deberá incluir como mínimo:

- una descripción sistemática de las operaciones de tratamiento previstas y de los fines del tratamiento, inclusive, cuando proceda, el interés legítimo perseguido por el responsable del tratamiento.
- una evaluación de la necesidad y la proporcionalidad de las operaciones de tratamiento con respecto a su finalidad; c) una evaluación de los riesgos para los derechos y libertades de los interesados o sujetos de los datos.
- las medidas previstas para evitar y afrontar los riesgos, incluyendo las medidas de seguridad y mecanismos que garanticen la protección de datos personales.

Pero haciendo caso al mismo artículo solo necesitarán realizar la evaluación de impacto, las empresas que cumplan una de estas tres casuísticas:

- evaluación sistemática y exhaustiva de aspectos personales de personas físicas que se base en un tratamiento automatizado, como la elaboración de perfiles, y sobre cuya base se tomen decisiones que produzcan efectos jurídicos para las personas físicas o que les afecten significativamente de modo similar;

- tratamiento a gran escala de las categorías especiales de datos a que se refiere el artículo 9, apartado 1, o de los datos personales relativos a condenas e infracciones penales a que se refiere el artículo 10,

- observación sistemática a gran escala de una zona de acceso público.

En nuestra PYME, que describiremos en detalle en el tercer capítulo, adelantamos que no va a cumplir ninguno de estos tres motivos, por lo que no estará obligada a la realización de la EIPD.

2.2 Registro de las actividades de procesado y tratamiento

Acorde Artículo 30 apartado 5: Las empresas de menos de 250 trabajadores estarán exentas de este registro. Es importante tener en cuenta que una misma empresa puede actuar tanto como responsable y como encargada al mismo tiempo, en función de los datos personales que maneje. Según la definición en el Reglamento:

- «Responsable del tratamiento» o «responsable», es la persona física o jurídica, autoridad pública, servicio u otro organismo que, solo o junto con otros, determine los fines y medios del tratamiento. Que en la versión en inglés del Reglamento correspondería con el “Data Controller”.
- «Encargado del tratamiento» o «encargado» es la persona física o jurídica, autoridad pública, servicio u otro organismo que trate datos personales por cuenta del responsable del tratamiento. En la versión en inglés correspondería al “Data processor”.

El registro de las actividades de procesamiento de datos tiene que estar documentado y en es obligatorio también en modo escrito. Por lo que tendrá que constar tanto en formato electrónico, como por escrito. También tendrán que ser registradas las peticiones requeridas o solicitadas por los posibles clientes de la empresa si los tuviera, al igual que las solicitadas por las autoridades de supervisión comunitarias o de cada miembro de la UE.

Por ejemplo en el caso de actuar como responsable de los datos, en la parte del registro relativa a la descripción del procesamiento de datos personales, tendrá que registrar los siguientes campos acorde al Reglamento en su art. 30:

a) Nombre y detalles de contacto del responsable y el delegado de protección de datos (DPD);

b) Propósitos o motivos del procesamiento (finalidad de los mismos).
c) Descripción de las categorías de los individuos objeto del procesado o tratamiento ("interesados") y de las categorías de los datos personales.
d) Categorías de los procesadores;
e) nombre y detalles de contacto de estos procesadores

Junto a las medidas de seguridad tanto técnicas como organizativas.

f) Límites de tiempo para el borrado de las diferentes categorías de datos
g) Descripción de las medidas de seguridad tanto técnicas, como organizativas.

En el caso de actuar como encargado, solo los puntos requeridos por la normativa para este caso en el mismo artículo.

2.3 Transferencia de datos a nivel internacional

Otro punto que obliga la normativa, pero que en nuestro caso también evitaremos tener que desarrollar, para facilitar este TFM, pero que obliga el nuevo Reglamento es el de la transferencia de datos a nivel internacional y que trata en su capítulo V, en los artículos del 44 al 50 del Reglamento.

En dichas transferencias internacionales de datos, lo importante será cómo escoger el lugar dónde ubicaremos los servidores y los accesos remotos, y la elección de las empresas subcontratadas para poder trabajar con éstas sin incumplir el Reglamento.

Los mecanismos de transferencia, para determinar el mejor método de transferencia de datos con otros países, se podrían realizar mediante los siguientes métodos:

.- Cláusulas contractuales estándar de la UE.
.- Normas Corporativas Vinculantes o BCR ("Binding Corporate Rules").
.- Códigos de conducta, cómo refleja el art. 40 del Reglamento.
.- O los conocidos escudos de privacidad ("Privacy Shields") desarrollados expresamente para la protección de datos entre países del continente europeo y americano.

2.4 Elección de un delegado de protección de datos.

Acorde a la sección 4 capítulo IV, artículos 37 a 39 del Reglamento, se describe la nueva figura del DPO (Data Protection Officer) o DPD Delegado de protección de Datos. La elección y nombramiento de este delegado no es obligatorio, solo en los casos, que marca el apartado uno del artículo 37, resumidos a continuación:

1.- El tratamiento lo lleve a cabo una autoridad u organismo público

2.- Las actividades de tratamiento requieran una observación habitual y sistemática de interesados a gran escala o
3.- las actividades principales consistan en el tratamiento a gran escala de categorías especiales de datos personales con arreglo al artículo 9 y de datos relativos a condenas e infracciones penales a que se refiere el artículo 10.

Pero, comentar que a pesar de no ser obligatorio, es más que recomendable por la importancia que cada vez se está dando a la protección de datos a nivel mundial y por la complejidad cada vez mayor en los sistemas de información o (IT) y por la necesidad de conocer el contexto legal del nuevo Reglamento, vamos a recomendar la elección de esta nueva figura para las empresas, que necesita de unas cualidades profesionales y conocimientos especializados del Derecho como experiencia en materia de protección de datos. Tendrá que desempeñar las funciones indicadas en el artículo 39 del Reglamento, que serán:

- Informar y asesorar sobre temas relacionados con la protección de datos;
- Garantizar y supervisar el cumplimiento, incluida la asignación de responsabilidades, concienciación y capacitación del personal involucrado en las operaciones de procesamiento y tratamiento, y las auditorías relacionadas.
- Proporcionar asesoramiento para PIA y controlar su rendimiento, que en nuestro caso particular no serán necesarios, ya que nuestra PYME no estaría obligada a realizar dichas evaluaciones de impacto, como comentamos anteriormente.
- Cooperar con las autoridades supervisoras de protección de datos, o sea, el comité Europeo de protección de datos, como las agencias de los estados miembros. En nuestro caso la AEPD (Agencia Española de Protección de Datos).
- Actuar como el punto de contacto para la autoridad supervisora. En nuestro caso la AGPD o AEPD.

La Comunicación si es probable que se produzcan infracciones de seguridad y el uso de un sistema de gestión de incidentes de seguridad, que también comentaremos en el punto cuarto y sexto, será también necesario implementar en nuestras PYMES.

2.5.- Introducción de las medidas de seguridad necesarias.

Este es la parte más técnica del TFM, donde veremos todos los cambios y adecuaciones que necesitará de expertos en el campo de seguridad informática y en redes. Entre las medidas a implementar, acordes con el artículo 25, que habla del concepto de la *"Protección de datos desde el diseño y por defecto"*, las más importantes serán las relacionadas con la protección de las bases de datos y de los ficheros que contengan datos de carácter personal, a parte se tendrá que exigir un mínimo nivel de seguridad en los servidores dónde estén alojados (bastionado de los servidores), podremos tener una políticas de accesos, para controlarlos, basada en roles y todas las comunicaciones con éstos servidores o con las bases de datos, deberá estar

cifrada, mediante protocolos seguros. A continuación expondremos las principales medidas de seguridad, técnicas y organizativas o de gestión:

- **La seudonimización y el cifrado de los datos personales**. Para ello analizaremos el estado de las últimas técnicas y recomendaciones en el campo de la seguridad IT. Por ejemplo la seudonimización la podremos implementar con métodos como las funciones hash o mediante tokens aleatorios.

Habrá que tener en cuenta que cuanto mayor sea el nivel de seguridad exigido, en función de la categoría de los datos personales a tratar, mayor será la dificultad de revertir el proceso de seudonimización. Así, el nivel de seguridad dependerá también de la finalidad del tratamiento de dicha información.

- **La capacidad de garantizar la confidencialidad, la integridad y la disponibilidad.**

Utilizaremos medidas como la encriptación de los datos y las comunicaciones. El uso de certificados como sistema de encriptado de las comunicaciones, mediante protocolos seguros como TLSv1.2 y evitar certificados auto-firmados y sin listas de revocación (CRL) o mejor que permitan el uso del protocolo en-línea OCSP, de control de certificados.

Para el control de accesos a los sistemas podemos utilizar, sistemas de código abierto con tecnología de árboles de directorios, basados en el protocolo LDAP (Lightweight Directory Access Protocol), que nos pueden proporcionar un sistema económico de autentificación y contabilización ("accounting") de los accesos.

- **La capacidad de restablecer la disponibilidad y el acceso a los datos personales de manera apropiada en el caso de un incidente físico o técnico.** Para conseguir un sistema que proporcione alta disponibilidad se pueden implementar técnicas de clusterización para alta disponibilidad (HA, "High Availability") en los equipos más sensibles y que procesen los datos personales y sistemas de repartición de carga (Load balancers).

En este apartado tendremos que añadir los sistemas de copias de seguridad o "backup" de los servidores y de las bases de datos, por ficheros (NFS) o bloques para poder recuperar los sistemas y los datos. Así conseguiremos que la probabilidad de pérdida de información sensible sea prácticamente nula. Un sistema fácil de implementar para realizar los backups y de bajo coste. También recomendaríamos, un sistema de recuperación frente a desastres (DR, "Disaster Recovery") el centro de datos de nuestra PYME.

Una política de copias de seguridad, que asegure la recuperación de los datos de la forma más rápida posible, será crucial para conseguir los niveles deseados de seguridad y evitar las indeseadas pérdidas de información.

- **Un proceso o procedimiento para probar y evaluar regularmente la efectividad de las medidas técnicas y organizativas que garantizan la seguridad del procesamiento**. Aquí podremos tener en cuenta algún método

de evaluación y certificación del bastionado o “hardening” de los servidores, tanto virtuales como “baremetal” o físicos. Un ejemplo podría ser el CIS-CAT aplicando el benchmark adecuado a cada equipo IT. La realización de auditorías y procesos de certificación de los sistemas IT, para verificar los niveles de seguridad se han de empezar a realizar en las PYMES que quieran cumplir con el Reglamento. También podemos utilizar métodos ya recogidos y aplicados en estándares o normativas como las ISO de seguridad y privacidad, para aplicar medidas de seguridad añadidas o un SGSI (sistema de gestión de la seguridad de la información).

Un sistema de gestión de incidentes y eventos de seguridad sería también recomendable, aunque no obligatorio, pero que nos ayudaría a cumplir con el reporte de los incidentes de datos, que comentamos a continuación, como por ejemplo, el de la norma ISO/IEC 27035:2011 [].

2.6 Notificaciones de violaciones de seguridad de los datos

¿Qué hacer si ocurre una violación de datos? Es una de las preguntas que a partir de ahora, se tendrán que hacer todos los empleados de una empresa y tendrán que tener muy clara su repuesta. Los artículos 33 y 34 nos dan las pautas, para que las empresas tengan en cuenta a la hora de implementar poder implementar este requerimiento de una forma adecuada.

Cuando se pueda haber producido una brecha en los datos (“data breaches”) o sea probable que ocurra, se ha de informar al delegado de protección de datos (DPD) o el departamento legal si se tiene o a un asesor de privacidad de inmediato como un Incidente de seguridad a través de alguna herramienta electrónica o digital si se tiene implementada.

El responsable tendrá que notificar antes de 72 horas el incumplimiento o violación de los datos personales a la autoridad supervisora competente, *“a menos que sea improbable que dicha violación de la seguridad constituya un riesgo para los derechos y las libertades de las personas físicas."*

Cuando es probable que resulte en personas físicas de alto riesgo, el controlador debe comunicar el incumplimiento de los datos personales al sujeto, excepto si ha implementado medidas apropiadas de protección técnica (por ejemplo el cifrado de los datos) y organizativas, o “*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.”*

Comentar, que existen particularidades, en este punto, para sectores concretos como el de las operadoras de telecomunicaciones, que son más restrictivas que el propio Reglamento de reporte. Estas empresas del sector de las telecomunicaciones, como por ejemplo las operadoras, están obligadas a informar en menos de 24 horas, estas incidencias de seguridad en los datos. Aunque, lo que realmente nos interesa, son las recomendaciones generales del

Reglamento, por lo que no entraremos en estos detalles, a no ser que cuando analicemos nuestra empresa sea necesario especificarlos.

2.7 Adaptación de los contratos para el cumplimiento del RGPD

Otra de las medidas a tener en cuenta, de carácter más legal y laboral, es el de La adaptación de los contratos al marco legal vigente. Los clientes de las empresas, que ejercerán como responsables de los datos y los de las empresas subcontratadas, que actuarán como encargadas del tratamiento (art. 28) deberán adaptarse, con nuevas cláusulas necesarias, que reflejen las nuevas exigencias relativas al tratamiento, procesado, normas de seguridad o responsabilidades sobre todo lo relacionado con los datos personales, así como los cambios exigidos por las mismas.

Esto llevará a que, los contratos se tendrán que evaluar y actualizar con los términos y condiciones actuales, tales como: protección de datos, seguridad y responsabilidad y tendrán que incluir nuevas cláusulas que reflejen los siguientes términos si son necesarios:

- En los nuevos contratos realizados antes de las EIPD si fueran necesarias, se tendrían que añadir cláusulas específicas sobre procesamiento de datos que necesitaran de EIPD.
- Justificación y alcance del procesamiento/tratamiento de los datos.
- Obligaciones de control y tratamiento de los datos necesarias para cumplir con el Reglamento.
- Violación de la seguridad de los datos personales y disposiciones por incumplimiento de la responsabilidad.
- Medidas técnicas y organizativas.

Además, se informará a los clientes, si nuestra empresa agrega o reemplaza a las empresas ya subcontratadas y se les informará de su derecho a oponerse a la elección de estas nuevas empresas subcontratas, que traten con nuestros datos personales.

2.8 Derechos del interesado

En este último punto de medidas, se recogen los derechos de los ciudadanos y residentes europeos, algunos ya contemplados en las actuales leyes de los países miembros de la UE, como la LOPD 15/1999 española [3]). En general se mantienen los antiguos derechos, pero reforzándose y haciéndose más estrictos en temas como: el acceso a los datos, la portabilidad de los datos, la retención de datos y el derecho a ser olvidado. Derechos que se recogen principalmente en las cinco secciones del capítulo tercero del Reglamento. Por ser uno de los capítulos fundamentales, vamos a repasar estos derechos por encima sin entrar en muchos más detalles que lo que comenta cada artículo y que tendremos que ver la forma de poder garantizarlos en nuestra empresa a estudio. En la siguiente guía, realizada por la AEPD se puede consultar en su cuarto punto, la explicación de cada derecho (guia-rgpd-para-responsables-de-

tratamiento [5]). A continuación comentaremos por encima todos los derechos que nos proporciona el Reglamento, a los afectados por el tratamiento de nuestros datos personales:

Transparencia y modalidades

Transparencia de la información, comunicación y modalidades de ejercicio de los derechos del interesado (Art. 12).

Información y acceso a los datos personales

Art. 13: Información que deberá facilitarse cuando los datos personales se obtengan del interesado
Art. 14: Información que deberá facilitarse cuando los datos personales no se hayan obtenido del interesado
Art. 15: Derecho de acceso del interesado

Rectificación y supresión

Art. 16: Derecho de rectificación
Art. 17: Derecho de supresión («el derecho al olvido»)
Art. 18: Derecho a la limitación del tratamiento
Art. 19: Obligación de notificación relativa a la rectificación o supresión de datos personales o la limitación del tratamiento
Art. 20: Derecho a la portabilidad de los datos

Derecho de oposición y decisiones individuales automatizadas

Art.21: Derecho de oposición
Art.22: Decisiones individuales automatizadas, incluida la elaboración de perfiles

Limitaciones

Art. 23: Limitaciones

A estos artículos añadiremos otros dos derechos importantes que son:

Art. 79: Derecho a la tutela judicial efectiva contra un responsable o encargado del tratamiento

Art. 82: Derecho a indemnización y responsabilidad

3. Descripción pyme. Tipos de datos personales y procesados

En este capítulo describiremos las características principales de nuestra empresa ficticia, a la que tendremos que aplicar todas las medidas necesarias para adaptarla al RGPD. Particularizaremos todas las medidas necesarias, recogidas en el anterior capítulo, para proteger los datos personales y garantizar los derechos de los sujetos según marca el Reglamento. Analizaremos y catalogaremos, todos los datos personales así como veremos el tratamiento que hace como responsable y como encargado (tratando los datos por cuenta del responsable).

La justificación principal, a la hora de escoger la empresa a estudio, es la de recoger las nuevas tendencias demandadas por las empresas que se están planteando o que ya están en una fase inicial en sus procesos de digitalización. El mundo empresarial, industria y sobre todo los sectores de las telecomunicaciones y el de las tecnologías de la información (TIC), está experimentando un período clave de cambio y tendencias cada vez más enfocado en la reducción de gastos y buscar soluciones más ágiles y duraderas en el tiempo. Intentan evitar cada vez más soluciones basadas en hardware propietario y poco flexible, que cada vez se quedan obsoletos o en desuso, por sus incompatibilidades con otros sistemas y proveedores, en un menor tiempo. Por eso, están optando cada vez más por soluciones basadas en nube y con la máxima virtualización posible, donde el hardware pasa a un nivel de importancia menor que el del software y las aplicaciones.

Las empresas necesitan reducir los costes existentes de implantación de los servicios y minimizar el tiempo de lanzamiento al mercado (TTM) de sus productos o servicios, para ofrecer a sus abonados, empleados o clientes, servicios cada vez más novedosos e innovadores. La virtualización estos servicios y productos es junto a la computación en nube, la técnica para reducir los costes de capital (CAPEX) y de operación (OPEX). La computación en nube es el modelo operativo que aprovecha su infraestructura para cumplir los objetivos de negocio y gastos de inversión de las pequeñas y medianas empresas, más limitadas en presupuesto, haciéndolas cada vez más competitivas.

Por ello, hemos escogido una pyme que ofrece servicios de nube privada del tipo básico, IaaS (Infraestructure as a Service) y de código abierto a sus clientes, para virtualizar uno de los servicios de telecomunicaciones más demandado y necesario por cualquier empresa, como es el de centralitas privadas (PBX) basados en técnicas de VoIP y virtuales (vPBX). El número de este tipo de centralitas virtuales en el mercado está creciendo exponencialmente en los últimos años.

Este servicio de nueva generación, de centralitas virtuales de voz sobre IP (VoIP) en nube, es el que explotará nuestra empresa para basar su negocio. Nuestra empresa pondrá la infraestructura para hospedar las PBX virtuales de las empresas que se lo soliciten, incluso podrá asesorar a sus clientes, y

recomendar algunos tipos de vPBX concretas, que ya estarán homologadas y certificadas por nuestra empresa para beneficio de ambas. Hemos escogido un modelo de infraestructura en nube, del tipo como IaaS, en el que se ofrecen máquinas físicas o acceso a máquinas virtuales para alquilar. Las empresas compran espacio en estos servidores y pueden instalar aplicaciones, usar el espacio de datos y realizar tareas en los servidores remotos de la infraestructura de la nube. Esto permite a una empresa externalizar sus propios centros de datos (DC). Los empleados de laas empresas hospedadas, solo necesitan un terminal que pueda conectarse a la nube. Para un mayor entendimiento de la empresa y de los servicios de VoIP virtuales se puede consultar la siguiente referencia relacionada con este tipo de empresas [6].

Para la parte de virtualización, hemos optado por un software estandarizado por la ETSI y compatible con la mayoría de aplicativos de este tipo. Están basados en la estructura que muestra la siguiente imagen, sacada de su web [7] y dónde se puede profundizar más sobre su arquitectura.

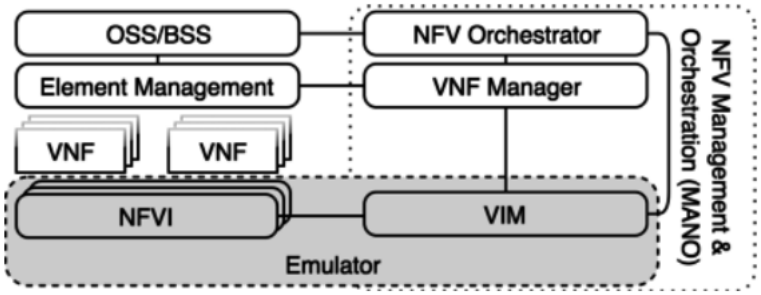

Ilustración 1.- Arquitectura simplificada de referencia ETSI NFV de virtualización.

La modularidad de la Arquitectura está diseñada para permitir que múltiples proveedores aprovechen los Estándares Abiertos sin estar encerrados en ningún proveedor en particular. Se espera que este concepto abierto impulse la estandarización continua de las API de acuerdo con las definiciones de la industria, ETSI en nuestro caso. La Infraestructura está diseñada para mantenerse al día con la evolución de la industria, estando al día con los Estándares Abiertos y las capacidades, al tiempo que se evita el bloqueo de proveedores individuales.

Podemos decir que lo que realmente ofrecemos es un servicio de IaaS, dónde los VNF, solo tendrán aplicativos virtuales de centralitas (vPBX) de VoIP, para pymes de menos de 250 trabajadores.

Las vPBX de VoIP, estarán basadas exclusivamente en el protocolo SIP (Session Initiation Protocol, descrito en [8]). Concretamente nuestra empresa ofrece su infraestructura para dar servicios de virtualización de centralitas de VoIP basadas en protocolos IETF. Podríamos catalogarlas como centralitas privadas virtuales para empresas, para más información ver la siguiente referencia [5].

Estas centralitas virtuales, son centralitas IP que funcionan en la nube que gestiona nuestra empresa, con lo que el cliente no tiene por qué tener en sus oficinas ningún equipo salvo los terminales, teléfonos IP o aplicaciones de

VoIP. Esta empresa ficticia, centra su negocio en las empresas pequeñas y medianas, que quieren tener un sistema telefónico avanzado y moderno, pero con una inversión y coste muy reducido. La nube privada que ofrece la empresa, para albergar a los clientes que quieran este tipo de centralita o "callcenter" virtual, aprovecharán todas las ventajas de la telefonía IP junto con las ventajas de trabajar en nube: ubiquidad, poder trabajar remotamente fuera de la oficina como si se estuviera en ella, etc.

Resumiendo, las ventajas que proporciona nuestra empresa ficticia, sería de gran interés para sus clientes, ya que recoge las ventajas de trabajar en nube, junto a las de virtualizar los servicios, que sumados tenemos como principales ventajas:

- Alta disponibilidad de los servicios, gracias a la infraestructura de la nube, junto a la virtualización del servicio. Se puede ofrecer duplicidad geográfica o georedundancia y clusterización de forma sencilla, para mejorar la disponibilidad de los servicios, integrados en máquina virtuales de fácil recuperación.
- Escalabilidad rápida y sencilla, únicamente provisionando más infraestructura virtual (VIM) para desplegar más VNFs con sus vPBX cada uno.
- Reducción del gasto, sobretodo en hardware dedicado, permitiendo a nuestros clientes aumentar en competitividad gracias a la reducción del CAPEX y OPEX, comentado anteriormente. Reduciéndose también los gastos en necesidad de infraestructuras y gastos de consumo eléctrico.
- Reduce el "time to market" de los servicios, forma rápida.
- Centralización de las operaciones de red, y mejorando la automatización de la red (network automation).

Nuestra infraestructura permite hospedar diferentes inquilinos (multi-tennant) que comparten la infraestructura, pero no los VNF, garantizando un aislamiento completo entre clientes, que serán responsables cada uno de sus datos. Nuestra empresa actuaria o ejercería el papel de encargado del procesamiento de los datos personales que se procesarán en su infraestructura, para cada vPBX. La Plataforma ofrece a los inquilinos herramientas para administrar todos los recursos físicos, virtuales, de forma autónoma sin depender de la administración de nuestra infraestructura.

Otras características de la infraestructura, será la de la automatización, permitiendo el despliegue, el aprovisionamiento y la administración del ciclo de vida para las vPBX, y además es Multi Hipervisor.

3.1 Características de la pyme para su adecuación al RGPD

Una vez descrita la plataforma de nuestra empresa, dónde ofrecerá los servicios a sus clientes, pasaremos a comentar otras características organizativas que nos servirán también para obtener las medidas necesarias para el cumplimiento del RGPD.

Con objeto de tener en cuenta la situación específica de las microempresas y las pequeñas y medianas empresas, el Reglamento incluye una serie de excepciones en diferentes puntos, que comentaremos más adelante, para organizaciones con menos de 250 empleados. Además, alienta a las instituciones y órganos de la Unión y a los Estados miembros y a sus autoridades de control a tener en cuenta las necesidades específicas de las microempresas y las pequeñas y medianas empresas en la aplicación del presente Reglamento. El concepto de microempresas y pequeñas y medianas empresas debe extraerse del artículo 2 punto 1, del anexo de la Recomendación 2003/361/CE de la Comisión Europea. Acorde a éste, tenemos:

1. La categoría de microempresas, pequeñas y medianas empresas (PYME) está constituida por las empresas que ocupan a menos de 250 personas y cuyo volumen de negocios anual no excede de 50 millones de euros o cuyo balance general anual no excede de 43 millones de euros.

De aquí que escojamos una pyme de menos de 250 empleados, para evitar que como responsable tengamos que cumplir con las tareas exigidas en el artículo 30 del Reglamento, en materia de registro de actividades de tratamiento. Para evitar también los registros como encargados del procesado de los datos, nuestra empresa no dará servicios a empresas con más de 250 empleados (250 abonados), ya que el responsable nos podría obligar por contrato a cumplir con esta obligación del Reglamento.

Otra característica sería el ámbito territorial en la que ofrece sus servicios y que también nos podría afectar a la hora del cumplimiento del RGPD. Por ello y para evitar procesados y tratamientos de los datos personales a terceros países, nos centraremos en el ámbito territorial de un mismo país de la Unión Europea (UE). Así como comentamos en el punto 2.3 de este trabajo, referente a transferencias de datos personales fuera de la UE, al no tener que transferir ni procesar datos fuera del ámbito de la empresa, ya que aunque podamos procesar una llamada de un empleado a otro empleado, siempre será el operador con tránsito internacional, el encargado de esta transferencia y nunca nuestra empresa.

Por último comentar que, nuestra empresa no tiene que tratar con datos bancarios, como son las tarjetas de crédito, por lo que evitamos tener que cumplir otras normativas relacionadas con este tipo de datos (bancarios) como la PCI-DSS, con rol de encargado de los mismos.

3.2 Tipo de datos personales como responsable y encargado

Para poder hacer un estudio de las medidas y requerimientos necesarios para adaptar nuestra pyme a la RGPD, es básico el análisis y clasificación de los datos personales de nuestra empresa. Por ello, a continuación pasaremos a describir los tipos de datos personales que tiene que tratar y procesar nuestra empresa a estudio. Para ello como ya hemos comentado anteriormente, los

dividiremos según el tipo de rol a la hora del tratamiento: como responsable (controller) y como encargado (processor) y posteriormente pasaremos a su clasificación. Es importante recalcar la diferencia entre datos personales e información confidencial de la empresa que en algunos casos pueden coincidir. Un ejemplo muy descriptivo que refleja esta diferencia sería, por ejemplo, el precio o presupuesto de un servicio, que por sí solo no da ninguna información personal, pero que es de carácter confidencial para la empresa.

- **Datos Personales como responsable**

Aquí tendremos los datos personales que encontramos en cualquier empresa, como pueden ser los datos de los empleados (dirección, DNI's, correos y teléfonos personales, números de seguridad social). Para más información podemos ver el siguiente documento de la Agencia de protección de datos española (AGPD-Guia_RelacionesLaborales2) [5], referente al tratamiento de los datos en las relaciones laborales como son los procedimientos de selección, la contratación, durante el desarrollo de la prestación laboral o en las relaciones con los representantes sindicales, que tienen muchas similitudes con el Reglamento.

Un caso especial seria el del DNI, dónde el RGPD en su artículo 87, da libertad a cada país de la UE a añadir medidas específicas para el tratamiento de estos tipos de datos identificativos, como son el DNI o el número de la Seguridad Social, que en nuestro caso a fecha de hoy no se han producido, por lo que de momento, no son necesarias medidas adicionales a las que marca el Reglamento. Aunque éstos son datos de categoría especial, el Reglamento nos permite su tratamiento, en el ámbito de la legislación laboral, como es nuestro caso.

Añadir también, que nuestra empresa no tratará con datos de carácter especial, recogidos en los artículos 9 y 10 del RGPD, fuera de los estrictamente necesarios por la ley laboral cómo hemos comentado. Ya que este tipo de datos, según la LOPD [3] requieren de un mayor nivel de medidas de seguridad y el Reglamento directamente los prohíbe de inicio, estableciendo nueve excepciones concretas, siendo así, todavía más restrictivo con éste tipo de categorías, respecto a la anterior legislación. Por lo que como no cumplimos ninguna de las nueve exenciones del artículo 9, no deberemos en ningún caso tratar con datos de categorías especiales como los religiosos o de afiliación sindical, entre otros.

- **Datos personales como encargado**

Como encargados de los datos de los clientes de nuestra empresa de servicios en nube con VNFs e inquilinos (tenants) relacionados con la virtualización de servicios de telefonía IP muy similares a una red IMS virtual, los datos personales a tratar serán los relacionados con el procesamiento de las llamadas de VoIP, o sea los descritos en el protocolo SIP de la IETF, descrito en la siguiente referencia [8]. De ahí, los datos que tenemos que procesar como encargados y no como responsables, están relacionadas con el tráfico de llamadas y más concretamente con el protocolo SIP. Por lo tanto, los datos

personales que debemos proteger acorde el RGPD, serán los relativos a este protocolo y que pueden identificar un sujeto, como marca el artículo 4 punto 1 y la anterior directiva sobre PII (Personal Identificable Information). Acorde a este protocolo, puede haber diferentes entidades de usuario, que coincidirán con los datos personales a proteger. Estos pueden ser el IMPI (IP multimedia private identity), el IMPU (IP multimedia public identity). Para más información sobre el protocolo SIP, ver referencia [8] de la bibliografía. Todos los datos anteriormente descritos, están clasificados como datos personales básicos. Las identidades de usuario, tendrán que ser tratadas entonces, como datos de carácter personal.

El único dato sensible, que podría tener que tratar nuestra empresa, si el cliente lo requiriera, es el de la localización, que SIP lo basa en el protocolo DNS o en el siguiente estándar [9], que añade una nueva etiqueta para este concepto: geolocation-sip. Aunque podría haber algún servidor de coordenadas si lo pidiera algún cliente tendríamos que contemplarlo en el momento que fuera necesario, para adecuarlo al Reglamento.

Las identidades de usuario SIP las trataremos con formato URI (uniform resource identifier) como por ejemplo: sip:michael.v@ejemplo.com. Las especificaciones de este formato URI han sido definidas en el estándar RFC 3986 [10].

Resumiendo, el tipo de datos personales que tendremos que tratar con el rol de encargados, serían principalmente los que nos permitieran identificas al abonado en cuestión, siendo de categoría básica, a excepción de los de localizaciones (más sensibles) y que estarían relacionados con el protocolo SIP.

Si se diera el caso en un futuro, por ejemplo, que nuestro sistema de VoIP tuviera que interactuar u ofrecer servicios específicos de IMS, tendríamos que añadir las identidades propias de la arquitectura IMS, como el GRUU (Globally Routable User Agent URI), que tuviera que procesar los sistemas de nuestra empresa, aunque sean solo en tránsito, como la señalización.

Nuestro sistema, por ser un sistema privado y con pocos abonados de VoIP, a diferencia de los sistemas IMS, no tiene una base de datos de suscriptores HSS, por lo que no tendremos identificadores del tipo IMSI, MSISDN, perfiles de servicio de suscriptor, activadores de servicios u otros datos, a tratar. Que tendremos en cuenta en el Capítulo 5 de la memoria, para implementar las soluciones que nos permitirán cumplir con el Reglamento.

- **Procesos y ficheros que podrían tartar con datos personales**

Otra parte importante, para desarrollar las medidas definitivas, para adaptar nuestra empresa, es hacer un análisis de los procesos y ficheros que podrían contener esos datos personales. En nuestro caso particular, podremos encontrarnos información de los abonados de nuestras centralitas en: registros de Sistema (logs), que siempre estarían activos por defecto, trazas de los protocolos de señalización, registros extraídos de operaciones de análisis de

fallos, según fueran necesarios (por ejemplo de un analizador de protocolos o de un sniffer de datos). Sería el caso, de necesitar extraer datos de abonado de la memoria RAM de una máquina virtual, por ejemplo, con fines de investigación, para solucionar algún problema (troubleshooting).

También podríamos encontrar datos personales, en trazas de software, registros de sistema, volcados de sistema o memoria, ficheros de tarificación, buffers de memoria o en simples ficheros del sistema operativo. Tendremos que contemplarlos todos, para asegurar que, nuestra empresa cumpla con el reglamento en cada caso descrito, que tenga la posibilidad de procesar este tipo de datos. Aunque, la gran mayoría de estos casos, serán procesados en memoria RAM (no permanentes o volátil) y en pocos caos en disco (permanente) como algunos registros de sistema. Nuestra empresa tendrá que analizar y evitar siempre que sea posible, los procesados y volcados en disco, o tomar las medidas necesarias, que marca el Reglamento, si son necesarios, para el correcto funcionamiento del sistema.

4. Medidas para adaptar la pyme al reglamento como responsables

Una vez descrita la empresa, y los datos personales que debe tratar o responsabilizarse de su protección, empezaremos a ver todas las medidas que debe tomar, acorde a los requerimientos del RGPD, y asegurar su completo cumplimiento. Este proceso de adaptación de nuestra pyme, podrá servir de ejemplo ilustrativo y didáctico, para otras pequeñas y medianas empresas, incluso sin ser del mismo sector.

En este capítulo, nos ocuparemos de las medidas necesarias que tendrá que implementar nuestra pyme, como responsable de los datos personales, comentados anteriormente en el punto 3.2, cuando tenga que procesar los datos personales, entendiendo por procesar, cualquier tipo de operación realizada en datos personales, por ejemplo, recopilación, grabación o almacenamiento, alteración, consulta, uso, divulgación, eliminación o destrucción, etc.

Comentar, que este capítulo a diferencia del siguiente, es más común o genérico al resto de empresas y por lo tanto, se puede encontrar más información en las guías ya comentadas como la de la AGPD en [5] y la de la Comisión Europea [11]. Por eso solo comentaremos las medidas, que sean de obligado cumplimiento para que nuestra pyme cumpla con el RGPD. Comentaremos sin entrar en detalle, la forma de implementarlas.

Añadir también, que hay medidas que se tendrán que ir revisando, ya que el Reglamento permite establecer normas más específicas mediante disposiciones legislativas o de convenios colectivos, que afectan exclusivamente al tratamiento en el ámbito laboral, que hasta la fecha no se

han producido, pero se tendrían que tener en cuenta en un futuro, acorde a los artículos 88 y 87, por ejemplo.

El artículo 9, referente al tratamiento de datos de categoría especial, como es el caso de nuestra pyme como responsable, para los datos de contratación por ejemplo, tipo DNI, o nº Seguridad Social, dirección del empleado, etc., no nos permitiría tratarlos, ya que los prohíbe por defecto. Pero permite excepciones siempre y cuando el tratamiento sea necesario para el cumplimiento de obligaciones, como el ejercicio de derechos específicos del responsable del tratamiento o del interesado en el ámbito del Derecho laboral y de la seguridad y protección social, como es el caso de nuestra pyme (apartado b). Al ser este nuestro caso, el Reglamento nos permitirá hacer uso o procesar este tipo de datos personales de categoría especial. En el considerando 52, también refleja lo comentado anteriormente, y en el considerando 10, incluso permite un margen de maniobra a los países de la UE, en el tratamiento de los datos de categoría especial:

(52) Asimismo deben autorizarse excepciones a la prohibición de tratar categorías especiales de datos personales cuando lo establezca el Derecho de la Unión o de los Estados miembros y siempre que se den las garantías apropiadas, a fin de proteger datos personales y otros derechos fundamentales, cuando sea en interés público, en particular el tratamiento de datos personales en el ámbito de la legislación laboral, la legislación sobre protección social, incluidas las pensiones y con fines de seguridad, supervisión y alerta sanitaria, la prevención o control de enfermedades transmisibles y otras amenazas graves para la salud.

10) El presente Reglamento reconoce también un margen de maniobra para que los Estados miembros especifiquen sus normas, inclusive para el tratamiento de categorías especiales de datos personales («datos sensibles»).

Dicho esto, a modo de justificación, pasaremos a enumeras las medidas necesarias de obligado cumplimiento, que tendrá que aplicar e implementar nuestra pyme como responsable directo de los datos, para adaptarse al RGPD.

4.1 Requerimientos de obligado cumplimiento para la pyme

En este apartado detallaremos los requerimientos de obligado cumplimiento por nuestra pyme, acorde al rol de responsable, que nos obliga el RGPD. Comentaremos también, los nuevos conceptos introducidos por el Reglamento europeo, que nuestra empresa tendrá que implementar para poder adaptarse. Los vamos a dividir en 7 bloques principales, parecidos a los comentados en el capítulo 2, pero adaptándolo al caso de una pyme, como la nuestra, para los datos personales ya comentados, en su mayoría provenientes de los empleados de la empresa, de sus clientes y de contactos de suministradores t proveedores.

4.1.1 Avisos y notificaciones

Nuestra pyme y todas las empresas que traten con datos personales han de garantizar, ya sea por correo electrónico o en algún documento, guía o manual de instrucciones para el cliente, que las declaraciones de privacidad aplicables se pongan a disposición de los interesados antes de o en el momento en que se recopilan los datos personales, que en nuestro caso normalmente coincidirá con una contratación de personal o de un nuevo suministrador.

El sujeto de los datos, como puede ser un abonado o un suscriptor de un servicio, debe estar informado sobre las prácticas de procesamiento de sus datos con respecto a cómo se recopilarán y usarán sus datos, y con qué fines. Este requerimiento de la RGPD está relacionado con los artículos 5, 6 y además en los artículos 13 y 14 se especifican los datos que han de contener dichas notificaciones, informaciones necesarias y la forma de hacerlo, según se hayan obtenidos los datos del sujeto. Estás notificaciones, las recomendaremos hacer vía documento, para dejar constancia escrita del acto.

- Notificación brechas de seguridad (art. 33 y 34)

Otro requerimiento importante que introduce el reglamento y que solo afecta a los responsables de los datos, es la de notificaciones de brechas de seguridad, que para el caso de nuestra pyme, lo tendremos que realizar en la siguiente URL [14] de la AEPD. En el caso de encargados de los datos, no estaríamos obligados a realizarlas, sino que serían nuestros propios clientes los que tendrían que realizar dicha comunicación antes de las 72 horas desde su conocimiento (art. 33). Es solo para empresas, los sujetos afectados tienen otra forma de notificarlo a la agencia.

Añadir, que si fuera necesario, por haber un alto riesgo para los derechos y libertades de las personas físicas, el responsable del tratamiento, también comunicará al interesado sin demora indebida (art. 34). Para el caso de nuestra empresa, serían los propios empleados, o los datos de los contactos de las empresas subcontratadas o de clientes.

4.1.2 Recopilación de los datos

Un caso especial del artículo 13, sería el de la recopilación de datos personales de forma voluntaria. Si el interesado proporciona sus datos personales, por ejemplo, vía un formulario web, éste deberá permitir la identificación de los campos de datos obligatorios y voluntarios. Solo los campos necesarios para que el servicio funcione pueden ser obligatorios su recopilación. En nuestro caso al igual que en punto anterior, serán los datos necesarios

Si el interesado proporciona sus datos personales, a través de un medio electrónico como puede ser un formulario web (tipo POST), el sistema deberá permitir la identificación de los campos de datos obligatorios y voluntarios. Solo los campos necesarios para que el servicio o producto funcione pueden ser obligatorios.

4.1.3 Comunicaciones a terceros

- Acuerdo de protección de datos personales

Cuando tenemos que encargar a terceras partes, como proveedores de servicios, el procesado de nuestros datos personales, debe realizarse acorde al Reglamento, como así reflejan los artículos 24, 24,28 y 32.

Este requisito tiene como objetivo transferir la responsabilidad legal de la protección de datos a terceros cuando están involucrados en actividades de subprocesamiento de datos. Las actividades típicas de subprocesamiento subcontratadas a terceros son entre otras, del tipo: gestión del almacenamiento de datos personales, solución de problemas y operaciones de atención al cliente basadas en datos personales (que en el caso de nuestra pyme no será necesario) o gestión de relaciones con clientes y actividades de marketing.
La guía del usuario de privacidad, que recomendaremos tener en nuestra empresa podrá tener información sobre la existencia de dichos terceros y su propósito de procesamiento de datos, ya que podría ser relevante para los servicios administrados, por ejemplo si tenemos contratado algún tipo de contrato de soporte o de operación y mantenimiento de alguna aplicación o SW o producto.

Las empresas deberían tener sistemas para gestionar los acuerdos de contratación de sub-procesados con terceras partes, acordes al nuevo marco regulatorio. Por lo que nuestro departamento jurídico, puede proporcionar una plantilla de acuerdo, para el abastecimiento de subprocesamiento por terceros, que se utilizará para cumplir con este requisito.

4.1.4 Consentimiento y libre elección del sujeto sobre sus datos

- Consentimiento (explícito, no tácito) y libre elección

Otro de los cambios introducidos en la privacidad en el nuevo reglamento es referente al consentimiento, que ahora ha de ser explícito y no tácito, para poder procesar los datos personales, por cualquier empresa. La agencia de protección española lo califica como “inequívoco” en su guía [5].

El consentimiento no debe considerarse libremente prestado cuando el interesado no goza de verdadera o libre elección o no puede denegar o retirar su consentimiento sin sufrir perjuicio alguno, acorde al considerando 42 del RGPD. Las condiciones del consentimiento se describen en el artículo 7 del Reglamento.

Para cumplir este requerimiento, nuestra empresa necesitará tener firmado todos los consentimientos o tener una prueba que garantice ese consentimiento.

Referente a la libre elección (artículos 7, 16, 17, 21 y 22), el interesado (en nuestro caso empleados, clientes o suministradores) se le ofrecerá con las

opciones y mecanismos adecuados, para mantener sus datos actualizados, realizar modificaciones o solicitar su eliminación, por parte de nuestra pyme.

- Exportación e importación de los datos (portabilidad datos personales)

Acorde a los artículos 15 (derecho de acceso del interesado) y 20 (portabilidad de los datos) del reglamento, se deberá soportar la exportación de datos personales, seleccionados en un formato estructurado, de uso común y lectura mecánica de forma segura. El objetivo de este nuevo derecho es capacitar al interesado y darle un mayor control sobre los datos personales que lo conciernen y poder tener acceso a ellos de una forma legible y estructurada.

Según la siguiente referencia [12], la definición que se hace de lectura mecánica ("machine-readable") por la European Union Law, es la de un fichero de datos en un formato que una computadora pueda leer y procesar automáticamente, como son los formatos CSV, JSON, XML, etc. Los "machine-readable" deben ser datos estructurados. Por ejemplo los archivos pdf, son "human-readable" pero no automáticos, ya que no están estructurados. Los documentos codificados en un formato de archivo que limite el procesamiento automático, y que los datos no puedan extraerse fácilmente de ellos, no deben considerarse de este tipo.

Los términos "estructurado", "comúnmente utilizado" y "lectura automática" son un conjunto de requisitos mínimos que deberían facilitar la interoperabilidad del formato de datos proporcionado por el responsable. Ejemplos de estos formatos podrían ser: VCard (para tarjetas personales electrónicas), RDF, CSV, XML, TXT, etc.

La viabilidad técnica de la exportación debe evaluarse caso por caso en las EIPD, que en nuestra pyme no estamos obligados a realizar como veremos. La viabilidad no debe crear la obligación de adoptar o mantener sistemas de procesamiento que sean técnicamente compatibles.

Estos supuestos deben reflejarse en la documentación o en la guía de privacidad del usuario del producto o servicio para el manejo de datos, de modo que se le advierta al cliente cómo cumplir con las solicitudes de portabilidad de datos. Para profundizar en el tema de la portabilidad recomendamos la siguiente referencia de la Comisión Europea [13], en ella se definen los siguientes tipos de datos para la portabilidad:

Datos personales seleccionados:
- Datos proporcionados de forma activa y a sabiendas por el interesado, por ejemplo un suscriptor o abonado (por ejemplo, nombre, dirección postal, nombre de usuario, edad, número de teléfono y otros datos personales básicos).
- Datos observados proporcionados por el interesado, p. un suscriptor, en virtud del uso del servicio de comunicación (voz o datos) o del dispositivo.

Ejemplo de datos en el ámbito de la aplicación:
-Registros telefónicos (por ejemplo, CDR), mensajes interpersonales o registros de VoIP, historial de la cuenta del suscriptor, llamadas y llamadas entrantes y salientes llamadas. Esto incluye todos los datos observados sobre el suscriptor durante las actividades para las cuales se recopilan los datos, como un historial de transacciones o un registro de acceso. Los datos recopilados mediante el seguimiento y la grabación del suscriptor (como una tecnología utilizada para rastrear el comportamiento de navegación o el historial de ubicaciones) también deben considerarse como "proporcionados" por él o ella, incluso si los datos no se transmiten activa o conscientemente.

Datos expresamente excluidos:
- Datos concluidos o derivados creados por el producto sobre la base de los datos "provistos por el interesado".

En general, si el valor de exportar los datos para el interesado, por ejemplo un suscriptor es insignificante, los datos pueden ser excluidos, por ejemplo:
- Si el abonado, se asigna a un determinado segmento de mercado en un sistema de CRM, en función de su comportamiento de navegación, los datos relacionados con el segmento de mercado no son elegibles para la portabilidad.
- Entradas de registro realizadas a propósito de la solución de problemas o la restauración del sistema.

- Restricción de procesamiento

Acorde al artículo 18, La restricción es una limitación del consentimiento dado previamente por el interesado al responsable (por ejemplo, en un contrato). Nuestra pyme en principio no debería necesitar, ningún procedimiento extra ni solución, siempre y cuando como responsable de lo datos, solo recoja los datos estrictamente necesarios para ejercer o cumplir con la legalidad laboral de sus empleados y clientes. Aun así, comentaremos varios aspectos importantes sobre la portabilidad.

La restricción afectaría a bases de datos que contengan datos personales de interesados. Archivos de logs, que contengan datos personales, estarían fuera del alcance de este requerimiento. Se deberá documentar la forma para ejercer este derecho de forma clara y accesible para, en el caso que se necesitara, aunque como hemos comentado, en nuestro caso de debería hacerse nada siempre que la recolección de datos cumpla con

Ejemplos de éste derecho para documentar, serían el de bloqueo de ciertos servicios de un suscriptor, evitar el envío de marketing a un interesado, el de evitar realizar análisis en ciertos datos de un abonado, el de evitar la realización de informes de estadísticas o para marcar los datos de un suscriptor y así saber que sus datos están restringidos.

4.1.5 Uso, retención, eliminación y calidad de datos

- Calidad de datos personales (artículos 5 y 6)

El servicio que proporciona nuestra pyme deberá soportar el mantenimiento de la calidad de los datos, actualizando o borrando los datos personales incorrectos, ya que aparte de estar obligado por el reglamento, permitirá hacer mejores negocios y que los clientes de la empresa confíen más y quieran seguir teniendo relaciones comerciales con nuestra empresa. Para ello es importante la "calidad de los datos", procesando los datos adecuadamente, legalmente y actualizados, rectificando o eliminándolos cuando sea necesario.

- Retención de datos personales (artículos 5 y 6)

Los datos personales, no se deberán guardar por tiempo indefinido, sobre todo si son de categoría especial como en nuestro caso. Por ejemplo siempre que se rescinda un contrato laboral o con un cliente, borraremos todos los datos relacionados con los mismos. Si se quisieran mantener durante más tiempo por causa justificada, los anonimizaremos correctamente. Así nos aseguraremos cumplir con el Reglamento. También deberíamos implementar un sistema para permitir el borrado programado o la anonimización de datos personales, aunque no es el caso de nuestra pyme, de acuerdo a los tiempos de retención de los datos que se necesiten borrar de forma programable, siempre que fuera necesario. Los interesados deben tener derecho a que sus datos personales se supriman y dejen de tratarse si ya no son necesarios para los fines para los que fueron recogidos o tratados de otro modo, si los interesados han retirado su consentimiento para el tratamiento, por ejemplo.

- Identificación de datos personales

Poder identificar los datos personales, nos permitirá buscar, modificar, borrar o anonimizar los mismos. Para ello necesitaremos aplicar técnicas de identificación de los mismos, que nos permita su clasificación y detección más rápidamente y poder tratarlos y procesarlos de una manera más eficiente. Un posible método sería el etiquetado de los datos, con las ventajas y desventajas, que suponen. El empleo de etiquetas, en comparación con otros sistemas de identificación, es más flexible y resulta especialmente sencillo. Podremos separar los datos personales del resto de datos, de una manera más sencilla permitiendo un procesado (búsqueda, extracción, borrado, anonimización, accesibilidad,…) más eficiente de los mismos, con sólo modificar sus etiquetas. Técnica muy útil en caso de que una persona interesada solicite saber qué datos personales tienen del mismo o si se pidieran por una de las autoridades o agencia de protección, para una posible investigación.

- Clasificación de los datos personales

Las empresas deben identificar por servicios o productos, que datos personales necesitan procesar, para poder evaluar su impacto en la privacidad y así poder aplicar las medidas de seguridad y procesos de privacidad, documentación y evaluaciones necesarias. Este requerimiento nos permitirá justificar o demostrar el Nuevo concepto de responsabilidad proactiva y qué categorías de datos personales procesa el producto y sus diferentes niveles de sensibilidad.

Además la clasificación de los datos debe permitir el cambio de la clasificación cuando se trabaja con diferentes entornos legislativos en empresas que trabajan con diferentes países y continentes, por lo que la empresa tiene que poder adaptarse a las diferentes legislaciones y definiciones de los datos personales, en el caso que fuera necesario, cuando ofrece el mismo servicio en diferentes marcos regulatorios.

4.1.6 Medidas de Seguridad para la protección de los datos personales

Este requerimiento se deriva de los artículos 24 (Responsabilidad del responsable del tratamiento), Artículo 25 (Protección de datos desde el diseño y por defecto) y del artículo 32 (Seguridad del tratamiento). Los vamos a dividir en las siguientes medidas que implementaremos en nuestra pyme.

- Derechos de acceso para la privacidad

La empresa debe asegurar, que solo el personal que tenga un motivo válido para acceder a los datos personales debería poder hacerlo. El acceso se proporcionará acorde la necesidad de conocimiento, solo para el personal específico que debe realizar una determinada tarea con los datos personales y solo para un conjunto específico de datos personales que deben conocerse, en nuestra empresa emplearemos un sistema basado en roles RBAC (Role Based Access Control).

Así, debe implementar el control de acceso y la gestión de derechos de acceso adecuados para que el administrador de privacidad, que podría ser el mimo delegado de protección, pueda definir perfiles de autorización y establecer permisos para los usuarios que tienen acceso a datos personales para realizar sus tareas, configurar a un usuario autorizado a qué datos personales se le permite el acceso, en función de la clasificación hecha y configurar y mostrar un mensaje de información a un usuario autorizado para recordarle sobre el secreto profesional (aviso bienvenida con un simple banner) y los acuerdos de confidencialidad al acceder a los datos personales.

- Confidencialidad e integridad de los datos personales

La RGPD, nos obliga a que los datos personales estén protegidos, para evitar brechas de privacidad y las temidas multas por parte de las autoridades de protección de datos. El uso del cifrado o criptografía es una forma efectiva de cumplir este requisito.

Se deberá proteger la integridad y la confidencialidad de los datos personales procesados por el producto, entendiendo por procesado cualquier operación o conjunto de operaciones que se realice con datos personales, por medios automáticos o no, como por ejemplo, la recopilación, grabación, adaptación o alteración, recuperación, consulta, uso, divulgación por transmisión, eliminación o destrucción, etc.

- Otras medidas de seguridad.

Para poder garantizar la seguridad que nos obliga tener el RGPD, sobre todos los ficheros, bases de datos que tienen datos de carácter personal, estaremos a tomar medidas concretas sobre esos equipos y las comunicaciones y accesos sobre los mismos. Por ello, identificaremos las bases de datos que tengan este tipo de datos y le aplicaremos las medidas pertinentes de seguridad para las bases de datos necesarias como:

- Cifrar las comunicaciones con la base de datos, con un protocolo seguro de comunicación como TLSv1.2, mediante su correspondiente certificado emitido por una entidad certificadora de confianza (no autofirmado).
- Solo se pueda acceder mediante una contraseña fuerte y basado en roles.
- Las APIs que puedan acceder a ella también estén securizadas, via TLSv1.2.
- Los datos de la base de datos estén cifrados.
- El Sistema operativo que la alberga esté bastionado (hardening) con un nivel de cumplimiento, por encima del 90%.
- Reglas de firewall para proteger los puertos de acceso a la base de datos.
- Redundar la base de datos y realizar las copias de seguridad periódicamente.
- Activar los registros de seguridad y acceso a la base de datos.

Para el caso de ficheros, serían muy parecidos. Todas estas medidas las añadiremos a las guías y políticas de seguridad nuestra empresa.

4.1.7 Responsabilidad proactiva y privacidad por diseño

Dos de los requerimientos o medidas incorporadas por el Reglamento son el de la responsabilidad proactiva ("accountability", art. 5): El responsable de los datos tiene que ser capaz de demostrar la improbabilidad de que la violación de la seguridad de los datos personales entrañe un riesgo para los derechos y las libertades de las personas físicas. Este nuevo concepto está muy relacionado con las EIPD (art 35), comentadas en el capítulo 2. Y el otro es el de la privacidad por diseño (art 25) que incluye medidas como la seudonimización o anonimización y la minimización de los datos. Ambos requerimientos los conseguiremos en nuestro caso con las medidas de seguridad comentadas en el apartado anterior.

4.2 Requerimientos de no obligado cumplimiento para la pyme

En los siguientes sub-apartados, comentaremos, los requerimientos que por las características de nuestra pyme, no estaría obligada a cumplir a diferencia de otras empresas.

4.2.1 Elección de un Delegado de protección de datos (DPD)

Como ya hemos comentado, aunque el RGPD contempla excepciones que nuestra empresa cumple, por lo que no sería de obligado cumplimiento, creemos conveniente la implantación de esta figura en nuestra pyme, por las

ventajas y mejoras que nos aportará en el cumplimiento. Tanto como responsables, como encargados.

4.2.2 Informe de evaluación de impacto de la privacidad (EIPD)

Según el Reglamento, las Evaluaciones de impacto de la protección de datos, solo son necesarias para los responsables y no son obligatorias más que en los supuestos, que marca el artículo 35, en sus apartados 1 y 3. Nuestra empresa, como responsable, al no cumplir ninguno de ellos, está exenta de realizarlos.

Cada producto, servicio y solución debe tener un informe de Evaluación de Impacto de Privacidad como parte de la documentación del producto. El informe incluirá la clasificación de datos personales con cálculo del índice técnico de privacidad, riesgos de privacidad y recomendaciones para la mitigación.

Los EIPD, ayudan a identificar y reducir los riesgos de privacidad. Se debe elaborar un informe para nuevos productos, servicios y soluciones. Son una forma de garantizar que se cumplan los requisitos básicos de protección de datos. El informe para un producto debe tener un alcance limitado al producto que se evalúa. El informe para una solución debe cubrir la solución global y su procesamiento extremo a extremo de los datos personales.

La entidad certificadora ISO, tiene guías para realizar estas evaluaciones como podemos ver en la siguiente referencia de la ISO 29134 [15], previo pago.

4.2.3 Registro de privacidad

El registro de las actividades de tratamiento, acorde al artículo 30 punto 5, por ser una pyme de menos de 250 empleados, estaríamos exentos de cumplirla, pero por las ventajas a nivel de seguridad y control, creemos conveniente realizarlo. Para ello nos podemos desplegaremos un sistemas centralizados de recogida de registros y eventos.

Las empresas deben poder monitorizar los eventos relacionados con la privacidad mediante logs que incluyan información relacionada con el procesamiento de los datos personales y que su acceso esté limitado por ejemplo al rol de administrador de privacidad, entre los que estaría incluido el DPD. Además deberá ser posible acceder a los eventos de privacidad, por ejemplo, usando etiquetas y no deberán contener datos personales reales a menos que esta información sea necesaria para ofrecer el servicio o la resolución de problemas.

El registro es importante para tener evidencias que se puedan utilizar en auditorías, por ejemplo, o en el caso de una violación de la privacidad para identificar las responsabilidades y las causas de la infracción en sí. Además, es importante que, cuando sea posible, los registros no incluyan información personal. De lo contrario, los archivos de registro también se convertirán en datos personales y deberán tratarse con el mismo nivel de protección que los otros conjuntos de datos personales (por ejemplo, cifrándolos).

Los registros de eventos de privacidad se pueden combinar con registros de eventos de seguridad, y los registros relacionados con eventos de privacidad (por ejemplo, registros de aplicaciones) deben seguir los requisitos de registros de eventos de seguridad genéricos existentes. Recomendaremos para nuestra empresa, registros que incluyan:

- Quién accede a datos personales.
- Marca de tiempo del acceso.
- Acciones o comando realizado sobre los datos personales.
- Sin datos personales reales.
- Etiqueta de privacidad.

4.2.4 Adaptación de los contratos para el cumplimiento del GDPR

Para el caso de nuestra pyme, como responsable, no necesitará adaptar los contratos, ya que no tiene que tratar datos personales, fuera del ámbito estrictamente laboral, a diferencia que como encargado a cuenta de otro responsable, que sí necesitaremos adaptarlos, como veremos en el capítulo cinco de la memoria.

4.2.5 Documentación relacionada con la protección de datos

El producto debe tener una guía del usuario de privacidad o de protección de datos personales como parte de la documentación entregada al cliente, aunque en nuestro caso, como responsable, al no tener clientes sería solo para empleados, donde reflejen de forma sencilla y clara, los derechos y la forma de actuar ante las incidencias, entre otros temas. La guía del usuario de privacidad debe cubrir los procedimientos para operar las funcionalidades de privacidad del producto, que como en nuestro caso no tenemos ningún servicio como responsable de los datos personales, no tiene sentido su elaboración como responsable.

Aunque tampoco es de obligada realización, también recomendaremos la elaboración de un código de conducta, según el artículo 40, así como posibles normas vinculantes corporativas como responsable o como encargado, recogidas en el artículo 47.

5. Medidas para adaptar la pyme al RGPD como encargados

Este es el capítulo principal, por su mayor esfuerzo de análisis y en el que menos información se puede encontrar, por la particularidad del servicio ofrecido y que por lo tanto aporta más valor a este trabajo y que puede servir de guía o ejemplo para otras pymes, incluso sin ser del mismo sector. Ya que nuestra empresa solo ofrece servicios como encargado y no como responsable, como ya hemos visto.

Destacar, que el RGPD, ha cambiado la figura o rol del encargado, dándole más importancia y asignándole un mayor número de obligaciones, que la anterior directiva no contemplaba (Directiva 95/46).

Según el RGPD, el responsable deberá adoptar medidas apropiadas, incluida la elección de encargados, de forma que garantice y esté en condiciones de demostrar que el tratamiento se realiza conforme el RGPD (principio de responsabilidad activa). Esto supone que todos nuestros clientes a partir de ahora nos exigirán ese compromiso, de ahí lo importante de adaptase al Reglamento.

En este capítulo entramos en detalle de las medidas a tomar por nuestra empresa particular, descrita en el capítulo 3, para adaptar nuestra empresa a la RGPD, en su papel de encargada del tratamiento. El tipo de datos personales que tiene que procesar nuestra empresa, son:

.- Datos dinámicos, relacionados al proceso de registro del protocolo SIP i que se eliminan una vez se des registra el subscriptor. O el de datos relacionados con una sesión, que se borran cuando se acaba.

.- Datos necesarios para solucionar problemas, recogidos de la señalización y cuando no hay actividad a nivel tanto del sistema como del abonado.

.- Datos para tarificación de las llamadas o sesiones.

.- Datos de señalización en tránsito para enrutamiento, control de sesión (algunos datos recién transferidos) y tarificación de las sesiones/llamadas SIP.

Comentar que al ser un sistema basado en VoIP, sin base de datos de abonados o HSS, no tendremos datos semipermanentes, que se borran una vez se ha des-registrado el abonado, ha expirado el tiempo máximo de registro o se ha bloqueado el servidor.

Una vez descritos los tipos de datos personales que trata nuestra empresa como encargado de los datos y el tipo de procesamiento de los mismos, ver también el apartado 3.2 de esta memoria, enumeraremos todas las medidas que estaremos obligados a aplicar para cumplir con los requerimientos del Reglamento y las que no. Empezaremos por las que no estamos obligados.

5.1 Requerimientos que no son necesarios aplicar a nuestra pyme

Las centralitas virtuales que se desplegarán en la nube privada de nuestra empresa, no proporcionan interfaces directos con los abonados del servicio, por lo que, al no tener un portal web, por ejemplo, dónde se puedan conectar los abonados directamente, nos evitamos tener que cumplir con los siguientes requerimientos:

.- Capacidad para apoyar la recopilación y demostración del consentimiento del sujeto de datos según los artículos 5, 6, 7 y 8.
.- Necesidad de presentar declaraciones de privacidad al sujeto de datos según los artículos 6, 13 y 14.
.- Gestión de consentimiento para la creación de perfiles y el uso de cookies (art: 14, 15).

Además acorde a los artículos 9 y 25, sobre la clasificación configurable de los datos personales, tampoco tendremos que tomar ninguna medida adicional, ya que nuestro producto o servicio, no tiene que administrar los datos de los abonados, los gestiona directamente la empresa que contrata nuestros servicios, que ejercerá de responsable de esos datos. La legislación y jurisprudencia de momento siempre es la misma, al operar solo en un mismo país, por lo que no hará falta cambiar la clasificación según el ámbito y país.

A su vez por el mismo motivo, ya que las aplicaciones que alberga nuestra nube en sus VNF y VIM, no tiene que proporcionar información de los abonados de las centralitas bajo petición, no tendremos que proporcionar acceso a los datos personales relacionados con un abonado bajo petición, según los artículos 13, 14 y 15.

Otro de los requisitos que tampoco necesitaremos cumplir, es el de ofrecer calidad de los datos (art 5 y 6), por no gestionar información personal. Los datos de los abonados, son los que nos proporciona el inquilino de nuestra nube.

El artículo 18, sobre la limitación del tratamiento, tampoco estará dentro de los requerimientos a implantar para adaptar la empresa al GPDR, ya que solo gestiona tráfico bajo petición (llamadas de los abonados) y si un abonado es dado de baja del servicio, nuestra empresa no deberá hacer nada más, ya que no podrá realizar llamadas ni otro tipo de acciones. Así, la suspensión del procesado de los datos personales del abonado, mientras mantenemos la información almacenada en nuestras bases de datos, no nos obliga a hacer ningún cambio adicional para cumplir este derecho.

En relación a lo anterior, tampoco tendremos que realizar ninguna medida adicional para cumplir con el derecho de portabilidad de los datos (art. 20) tanto para importar como exportar datos relacionados con el abonado, ya que los servicios de VoIP que gestionamos, no importan directamente datos de abonado, lo recuperan solo cuando lo necesitan durante los procedimientos de tráfico de llamadas o sesiones, como el registro o el establecimiento de sesiones SIP. Añadir que en el caso de actividades de solución de problemas

del servicio (troubleshooting), podría ser necesario el exportar datos del abonado en ficheros de registros o logs, pero únicamente en este caso, por lo que al final para asegurar el cumplimiento, aplicaremos medidas para el caso de la exportación de datos de los registros.

Por último no deberemos realizar una EIPD como encargados del tratamiento, ya que según el Reglamento en su artículo 35, es tarea exclusiva del responsable de los datos, en este caso las empresas que se alojan en la nube para instalar su vPBX. Por lo que estamos exentos de realizar y actualizar las EIPD acorde a los artículos 6, 24, 25 y 35.

5.2 Medidas necesarias para adaptar y cumplir el Reglamento

Cumpliendo el Reglamento conseguiremos proteger a los ciudadanos y residentes europeos de las violaciones en los datos personales y de privacidad.

1.- Etiquetado de los datos personales en los ficheros, logs acorde a los artículos 4, 5, 6, 9,17.

La identificación de los datos personales, por ejemplo, mediante el etiquetado de los datos personales en archivos de registros (logs), nos permitirá cumplir con otros requerimientos, como el de exportar datos de un formato adecuado y legible para otros sistemas. Para ello utilizaremos un etiquetado xml, con etiquetas de inicio y fin de datos. En el siguiente apartado lo veremos con más profundidad. Comentar, que como encargados del procesamiento, nuestra plataforma no gestiona bases de datos de cliente, no hará falta identificar ningún otro dato más que los generados en logs o archivos de sistema, principalmente.

2.- Exportar datos personales relacionados con un abonado en un formato estructurado, de uso común y legible por máquinas (“machine-readable”).

En nuestro caso la importación de datos a la infraestructura, no es necesaria, porque es el propio cliente el que gestiona sus abonados.

Esta medida de carácter técnico, nos obliga a etiquetar/identificar todos los datos personales comentados en el tercer capítulo, como el sipuri, y que necesitamos alinear siguiendo un procedimiento de etiquetado común en toda la plataforma y centros de datos de nuestra infraestructura. Para ello el etiquetado ha de ser simple y que nos permita obtener registros (logs) legibles. Como el Reglamento no exige ningún formato o técnica concreta, aunque podríamos usar un método basado en expresiones regulares, hemos optado por el de etiquetas específicas para cada dato personal y tipo. Por ejemplo para etiquetar un sipuri utilizaremos la nomenclatura tipo de los lenguajes de marcado como el xml. Vemos un ejemplo a continuación en el caso de un mensaje de registro de un abonado:

Request-Line: REGISTER sipuri: sip:michael.v@ejemplo.com SIP/2.0
Request-Line: REGISTER **<sipuri>**sip: sip:michael.v@ejemplo.com**</sipuri>**SIP/2.0

Donde vemos las etiquetas tipo xml añadidas al principio y fin del dato personal. Comentar que diferentes datos personales deben tener diferentes etiquetas, por ejemplo para el caso de datos de localización podemos utilizar las etiquetas de marcado <loc> </loc> a principio y fin del dato de localización. Así, las etiquetas que proponemos para los datos utilizados por los VNF de las vPBX, serán del tipo: “<sipuri> </sipuri>”, o “<loc> </loc>”.

Una vez etiquetados los datos personales, podremos exportar datos personales de nuestra infraestructura incluyendo los VNF con las etiquetas necesarias, para su posterior procesado y tratamiento. Los datos de los abonados pueden almacenarse en registros de sistema, o de trazas para realizar troubleshooting de señalización o del SW, registros de datos como los de tarificación si los demanda el cliente. Este último tipo de registros ya está etiquetado por defecto normalmente.

Una recomendación de diseño por defecto (art. 25) que también aplicaremos siempre, será la de **no almacenar datos en registros u otros sistemas, que no sean estrictamente los necesarios (“minimización de los datos”)**. Se verificarán todos los registros disponibles en cada VNF para analizar si tienen datos personales almacenados, y si la información ya está etiquetada o no. Al igual que en proveedores o terceras empresas de nuestra nube, como SW de terceros o servidores de análisis de estadísticas.

También describiremos todos los etiquetados necesarios por nuestra infraestructura en la guía de privacidad del usuario de nuestra empresa.

3.- Soporte para el borrado y la gestión de la retención de los datos (art. 5 y 6)

Eliminar todos los datos personales relacionados con un abonado, previa solicitud o a través de un tiempo de retención programado acorde al “derecho al olvido” descrito en el artículo 17. En nuestro caso incluso antes de haberse tramitado la baja del abonado al responsable de los datos de la centralita virtual. Este requerimiento lo conseguiremos gracias al etiquetado realizado previamente de todos los registros necesarios. También, asumiremos que los logs con datos personales no deben ser borrados por nuestra empresa ya que por diseño los tendremos controlados y centralizados en un servidor central.

Este requerimiento no es aplicable a cierta información como la de tarificación si la requiriese el cliente. La información de tarificación, debe ser almacenada hasta que pueda transferirse al sistema de facturación (billing system), que normalmente estará en las oficinas del cliente. Eso sí, como comentaremos más adelante, han de transferirse cifrados al servidor que gestiona la tarificación.

La configuración de la privacidad por defecto, como la del tiempo de retención predeterminado para los datos personales, establecidos por contrato o no. Así, los registros cada cierto tiempo se finalizarán y se eliminarán los datos o se sobrescribirán. Pero si no existe un contrato o directiva, sobre la periodicidad

del borrado, los registros se eliminarán después de un período de tiempo configurable. Una forma de implementar este requerimiento, es vía ficheros crontab de Linux, en todos los equipos “baremetal” o máquinas virtuales que procesen registros o ficheros con datos de abonado en nuestra plataforma.

4.- El siguiente requerimiento, que nos obliga a tomar más medidas técnicas, es el relacionado con la seudonimización de datos personales (art. 6, 25 y 32). Los datos que según el RGPD debemos seudonimizar en nuestra empresa, serán como hemos visto anteriormente en este capítulo los datos personales almacenados en los registros y en las bases de datos necesarias para el servicio.

Aunque en la parte de virtualización de la centralita (VNF) se pueden seudonimizar los datos personales, mediante técnicas de uso de claves, es la parte más complicada, porque tendremos que verificar en cada SW de cliente (vPBX) que no afecta a la funcionalidad del servicio, este cifrado de los datos, ni a nivel de introducción de latencias ni de fallos de procesado.

Una técnica sencilla y de fácil implementación para la seudonimización y que no afectaría al formato original del dato personal es la FPE (Format Preserving Encryption), aceptada por el organismo americano NIST (National Institute of Standards and Technology, ver referencia [16]) cómo algoritmo de cifrado de datos. Con esta técnica mantenemos el formato inicial de los datos, pero conseguimos seudonimizarlos acorde al Reglamento, para su posterior tratamiento. Lo ideal sería que cada cliente incluya ya este cifrado en sus programas, para que no tener que certificar cada solución de forma independiente.

Así por ejemplo nuestro sipuri podría quedar del siguiente modo, aplicándole una función fpe_encrypt():

fpe_encrypt (“michael.v@ejemplo.com”,tweak,clave) ---> hytgriw.m@frthnyu.rtg

Consiguiendo la anonimización del dato personal. Comentar que hay dos tipos de algoritmos FPE, el FF1 y el FF3 como se explica en [16], funciones ya implementadas en los lenguajes de programación y de fácil implementación. Tendremos que mantener el mismo algoritmo y reglas para el mismo tipo de dato en todo el sistema.

Así el funcionamiento normal será el de detectar las etiquetas de los datos personales para después anonimizarlos mediante el encriptado FPE, proceso que necesitaremos, en nuestro caso, para exportar los logs necesarios, para su tratamiento y cumplir con el RGPD.

Los diferentes tipos de logs que pueden contener datos personales en nuestra infraestructura y que tendremos que analizar para aplicarles el etiquetado y la seudonimización, mayoritariamente provendrán de registros de alarmas o alertas, registros de la aplicación, trazas de sistema o de la aplicación, que tendremos que analizar y etiquetar adecuadamente, para posteriormente poder seudonimizarlos. Comentar que normalmente el software debería ser agnóstico

a los datos registrados, como puede ser los datos de señalización y además suelen ir correctamente etiquetados y también el software de terceras partes tiene sus propios logs independientes de los estrictamente funcionales del servicio.

5.- Cifrado de datos personales almacenados y en tránsito.

Necesitamos cumplir otra medida técnica, para proteger los datos personales almacenados en memoria permanente, como obliga el RGPD. Para ello, restringiremos el acceso a los ficheros y bases de datos, mediante los permisos correspondientes a los registros que contengan datos personales, tanto logs que tengamos que exportar como ficharos de tarificación. También aplicaremos un control de acceso basado en roles (RBAC) a los que solo podrán acceder las aplicaciones que procesen los datos y nadie más, que comentaremos en el siguiente punto de medidas de cumplimiento.

A estas dos medidas, añadiremos encriptación de los datos mediante claves o certificados. Tanto a la parte de infraestructura que lo necesite como a los VNF. Por lo tanto, los VNF deberán también usar los permisos adecuados para evitar accesos no permitidos a los datos personales y además también encriptación de los datos y deberán seguir el mismo criterio en todos los VNF.

Para el caso de los datos en tránsito, caso de la señalización de las llamadas y servicios SIP, la solución será encriptar los interfaces por donde pasen datos personales, que serán todos por dónde pase señalización básicamente. Para ello, dos opciones de encriptado de estos interfaces serían: con IPSEC o con el protocolo de criptografía asimétrica o de clave pública TLS (Transport Layer Secure). Con ello cumpliremos con el Requerimiento de los artículos asegurando la privacidad, confidencialidad de los datos. Por motivos de mayor seguridad y por ser un protocolo de la IETF (ver la referencia [17]) de gran utilización e uso, en su versión 1.2, que es la más segura hasta la fecha. Este punto nos puede limitar a tener que denegar servicios a clientes que sus aplicativos de vPBX (VNF) no soporten este protocolo seguro de comunicaciones. En la parte de las comunicaciones de la señalización interna del VNF también se puede plantear el uso de este protocolo, aunque no tiene la prioridad de los interfaces de señalización externos.

6.- Control de acceso basado en roles para archivos con datos personales. Acorde a los artículos 24, 25 y 32.

Para implementar el control de los accesos a los ficheros, registros o bases de datos que contengan en nuestro caso datos de identificación personales como sipuri's, IP's, etc. o datos de localización, por el Reglamento, hemos escogido una política de control de accesos basada en roles (RBAC) aplicando el principio de menos privilegio, en el que los usuarios de bajo nivel no deberían tener acceso a los datos personales, ya sean en ficheros de registros, como en bases de datos. En principio no necesitaremos ningún rol adicional. Ya que tanto el administrador del sistema, el administrador de la aplicación y los departamentos de soporte técnico que realizan el troubleshooting, pueden tener acceso a los datos personales, como hemos comentado anteriormente.

Este tipo de control de acceso se puede implementar con programas de código abierto que no requieren de una gran inversión.

La adaptación a la normativa por parte de nuestra empresa nos obliga a actualizar y desarrollar nueva documentación relacionada con la seguridad y las guías de usuario para nuestros clientes, dónde debemos reflejar todos los cambios introducidos en el procesado de los datos personales.

7.- Acuerdos de protección de datos con terceras partes (art: 24, 25, 28, 32)

Firmaremos contratos con terceras empresas que tenga que tratar datos personales de nuestros clientes, por ejemplo, con propósitos de troubleshooting, o análisis de volcados de memoria. Necesitaremos acuerdos contractuales, con estos sub-encargados del tratamiento de los datos, que podrán ser tanto terceras empresas que suministran software de código abierto tipo Red Hat (empresa suministradora de SW), Canonical, etc o de hardware como Dell EMC o HP. Los contratos con estas empresas subcontratadas, se tendrán que revisar para que cumplan con todos los requisitos que nos obliga la RGPD en el caso de nuestra empresa y que hemos analizado con anterioridad, al igual que los VNF de cada cliente, que las empresas de SW también cumplan el Reglamento.

5.3 Medidas recomendables pero no obligatorias para nuestra pyme

Como hemos comentado en capítulos anteriores (2 y 3), hay medidas o requisitos del Reglamento, que por nuestro tipo de empresa no estaríamos obligados a cumplir, pero que por la ventajas que nos van a aportar hemos decidido que son más que recomendables. A continuación las detallaremos:

1.- Elección de delegado de protección de datos

El artículo 37, solo obliga a tener un DPD, solo en el caso de 4 supuestos que no cumplimos, por lo que no nos obligaría a tener que designar un DPD en nuestra empresa, pero por la importancia que toma la privacidad y la protección de datos en el mundo de los negocios y en concreto en el sector de las telecomunicaciones, al que nuestra empresa pertenece, vemos conveniente su designación, aunque no sea en exclusividad y le permitamos desarrollar otras funciones, como así contempla el RGPD. Por lo que por razones de imagen empresarial y las ventajas que introduce por sus responsabilidades de control, supervisión y asesoramiento en la materia de la protección de datos y sobre todo por las dificultades y esfuerzos iniciales de la implementación de todas las medidas y los vacíos o dudas legales que existen todavía en algunos puntos del Reglamento, que permite leyes adicionales sobre esta materia de protección de datos a los países miembros de la UE, y que la AEPD o AGPD todavía falta pronunciarse.

2.- Formación y divulgación relacionada con la privacidad y el Reglamento

La realización por el delegado de protección de datos, de seminarios y sesiones divulgativas sobre privacidad y el Reglamento, principalmente a las personas encargadas o que han de tratar con estos temas en la empresa.

Cursos de formación específica sobre privacidad o sobre el Reglamento de protección, también impartidos por el DPD escogido.

3.- Registro de eventos de privacidad, relacionados con datos personales.

Aunque al igual que con la elección del delegado de protección de datos, por ser una empresa de menos de 250 trabajadores, el artículo 30 punto 5, nos eximiría del cumplimiento del registro de las actividades del tratamiento como encargados, aun no siendo los responsables de los datos de nuestra infraestructura de nube privada, pero por razones obvias de imagen, de seguridad y control de las actividades relacionadas con la privacidad, registraremos todas las operaciones de usuarios, que tengan que ver con o asociada a datos personales, como recuperación de registros, modificación de registros, eliminación de registros, recuperación de información específica de abonados, inicio y finalización de actividades de rastreo, y otras operaciones que se pueden realizar en el servicio relacionadas con los datos personales.

Para ello activaremos los registros y contabilización de todos los usuarios (user accounting) de la plataforma y equipos que tengan que procesar dichos datos personales, ya sea en ficheros, bases de datos, volcados de memoria, etc., y lo completaremos un sistema de registro centralizado, basado en protocolos seguros de transferencia, de los registros exclusivos que traten con datos personales, como pueden ser aplicativos de código abierto y de licencia GNU basados en rsyslog [18], o un por ejemplo, que permite comunicaciones cifradas vía TLSv1.2 durante el traspaso de los registros.

4.- Adaptación documentación de la empresa al RGPD

Otra medida de no obligada cumplimentación es el de la adaptación de la documentación existente o creación de guías de privacidad para usuarios. La creación de una guía de privacidad para los usuarios o clientes de nuestra nube, donde reflejemos los procesados realizados a los datos, así como el etiquetado y la seudonimización realizada a sus datos, la forma de acceder y los procedimiento para manejar los datos.

Otros documentos adicionales, serán el que recoja las directrices y política referente a seguridad y los cambios y medidas adicionales para la adaptación al Reglamento.

Las guías de bastionado (hardening) de los equipos, las actualizaremos también con las medidas necesarias para la protección de datos desde el diseño y por defecto.

Generar una guía de privacidad para los usuarios, dentro de los manuales que se entregan a los clientes que usan los VNF's de nuestra nube, para instalar sus centralitas virtuales de VoIP. Así podremos cumplir con los artículos 6, 13, 14, 25, 35.

5.- Subscripción a un CSIRT para la gestión y control de las vulnerabilidades

Para la gestión de las vulnerabilidades tanto de software principalmente, como hardware, recomendamos subscribirse a algún CSIRT, como podría ser el CSIRT de España [19].

5.4 Análisis de impacto e implementación de las medidas

Previo a la etapa final del proceso de adaptación de nuestra pyme, o de cualquier otra empresa, recomendaríamos realizar un análisis del posible impacto de las medidas tomadas, principalmente de las que puedan afectar al servicio y otros procedimientos o documentaciones de la empresa.

5.4.1 Análisis de impacto como encargados

Comentar que no hemos realizado el análisis de impacto como responsables, por no tener impacto directo en el servicio a los clientes, que es la parte principal para la empresa. Una vez dicho esto, por ejemplo, en nuestro caso particular analizado, tendríamos impacto en los siguientes puntos:

.- En los interfaces de señalización, al encriptarlos con TLSv1.2,
.- En las características de los datos personales, ya que ahora van estarán cifrados y seudonimizados.
.- En los registros (logs) con datos personales del sistema, ya que ahora hay que programar sus borrados también.
.- En la tarificación si la hubiera, pero no será nuestro caso.
.- Impacto en la seguridad, por la implementación del acceso por roles RBAC y la monitorización de eventos y en la conectividad por el uso de protocolos de comunicación encriptados seguros. Necesidad de conexión a una autoridad certificadora para revocar certificados (CRL) o gestión del protocolo OCSP
.- Impacto en los documentos de la empresa. Como las EIPD si las hiciéramos, que no es nuestro ya que no somos responsables de los datos. En las guías de privacidad y seguridad de la empresa y en las Guías de hardening de los equipos de la infraestructura de la nube.

En cambio no lo tendríamos en:

.- En la arquitectura de nuestro sistema
.- No habría impacto directo con abonados ni en su provisión, ya que la gestión la hace directamente el cliente, como responsable de los datos.
.- Ni en los estándares de Voz, como SIP.
.- En nuestro caso no tendremos Tampoco tendremos impacto en versiones anteriores de software.

.- Tampoco habrá impacto con las funciones propias de la vPBX, como los servicios complementarios del tipo tonos de llamada, conferencias a tres, etc.

5.4.2 Implementación de las medidas

Una parte importante que no hay que olvidar es el de la implementación de todas las medidas, sobre todo las técnicas, que podrían afectar al funcionamiento del servicio que ofrece nuestra empresa. Para ello, una vez especificadas las medidas, sobre todo las que necesitan de cambios a nivel funcional, como el etiquetado, la anonimización o las medidas de seguridad propuestas para la protección de los datos, necesitaremos realizar las pruebas de regresión necesarias, para certificar principalmente, que la funcionalidad no se haya visto afectada. Comprobaciones, Sanity checks, PoC (Proof of Concept) previos a las pruebas de regresión, también pueden ser necesarios, para realizar posteriormente las definitivas pruebas funcionales y la consiguiente certificación de los cambios en nuestra plataforma y sistemas informáticos, con la seguridad de que no van a haber problemas de última hora ni impactos en la funcionalidad del servicio.

Una vez realizadas las pruebas funcionales y los test de regresión, pasaríamos a certificar tanto la parte funcional como la de seguridad de nuevo. La Seguridad como la funcionalidad de la infraestructura y del servicio de las vPBX, no deberían verse afectadas por las medidas introducidas para adaptar la empresa al Reglamento.

6. Conclusiones

Este proceso de adaptación de nuestra pyme, tanto como responsable de los datos, como encargado, como hemos visto en detalle en los últimos capítulos de esta memoria, podrá servir de ejemplo ilustrativo y didáctico, para otras pequeñas y medianas empresas, incluso sin ser del mismo sector, a modo de guía o recomendación para que sean capaces de analizar y proponer sus propias medidas, para cumplir con el reglamento.

El principal objetivo que nos propusimos, el de extraer una serie de medidas, a partir de una lista de verificación o checklist, extraída de la lectura del Reglamento y de las guías propuestas de la Comunidad Europea y la AEPD, como puntos a cumplir, creemos que ha sido acometido, incluso añadiendo medidas no obligatorias, que hemos creído conveniente implementarlas en nuestra pyme.

Hemos analizado y recopilado todos los requerimientos que marca el RGPD para encontrar una forma viable y sencilla de implementarlos en nuestra empresa ficticia, tanto los técnicos como la identificación de los datos vía etiquetas, o la seudonimización con algoritmos FPE, como los organizativos como la elección del delegado, o la realización de guías de privacidad del

servicio, o la modificación de los contratos con terceros, siempre que sean necesarios y particularizándonos en nuestra empresa.

Recalcar, como hemos ido comentando a lo largo del desarrollo de la memoria, que la RGPD no acaba más que empezar su andadura, y que el Reglamento permite añadir más especificaciones a los organismos autorizados en cada país de la Unión, en nuestro caso la AEPD, por lo que el proceso de adaptación, nunca estará cerrado y tendrá que seguir adaptándose, conforme las agencias vayan introduciendo nuevos requisitos que crean convenientes.

Otra parte importante que no hemos olvidado, introducida al final de la memoria es la del análisis de los posibles impactos de la implementación de las medidas, aunque no se haya tratado en profundidad, a diferencia del estudio de la viabilidad económica de la implantación de los mismos, que no lo hemos tratado, ya que no era este nuestro objetivo ni tampoco el del Reglamento, por lo que no lo hemos tenido en cuenta en ningún apartado de la memoria. Aunque siempre se ha tenido en cuenta a la hora de implementar las soluciones de forma implícita. Hemos siempre intentado buscar medidas de fácil implementación y lo más sencillas posibles, sin por ello, dejar de cumplir con el Reglamento, buscando soluciones siempre de código abierto y no propietarias y cerradas, como por ejemplo para el control de los accesos por roles, el etiquetado o la seudonimización.

7. Glosario

API (Application Programming Interface): Interfaz de Programación de Aplicaciones. Es el conjunto de subrutinas, funciones y procedimientos que ofrece cierta biblioteca para ser utilizado por otro software como una capa de abstracción.

CAPEX (Capital Expenditure): Dinero que invierte una empresa en la mejora o adquisición de productos o servicios.

CRL (Certificate Revocation List): es una lista de certificados (concretamente sus números de serie) que han sido revocados y ya no son válidos.

CPD (Centro de procesamiento de datos): Lugar en el que se almacenan todos los recursos necesarios para el procesamiento de la información de una empresa.

CSIRT (Computer Security Incident Response Team): Es un centro de respuesta a incidentes de seguridad informática. Responsable del desarrollo de medidas preventivas y reactivas ante incidencias de seguridad en los sistemas de información.

DC (Data Center): Lugar en el que se almacenan los recursos físicos y lógicos necesarios, para el procesamiento y control de la información de una empresa.

IaaS (Infaestructure as a Service): Tipo de servicio en nube, en el que una organización vende la capacidad de procesado y almacenamiento, para que terceros implementen sus aplicaciones.

NFV (Network Functions Virtualization): Arquitectura de red que utiliza técnicas relacionadas con la virtualización de los servicios.

NFVI (NFV Infraestructure): constituye la base general de la arquitectura, contiene el hardware para alojar las máquinas virtuales, el software que hace posible la virtualización y los propios recursos virtualizados.

OCSP (Online Certificate Status Protocol): Protocolo de comprobación del estado de un certificado en línea. RFC 6960.

OPEX (Operational Expenditure): Dinero que invierte una empresa en el mantenimiento de los productos o servicios.

SDN (Software Defined Networking): Red Definida por Software. Tecnología que permite administrar los servicios de red mediante la abstracción del plano de datos.

SIP (Session Initiation Protocol): Protocolo de Inicio de Sesión.

VIM (virtual infrastructure manager): Gestor de la de la infraestructura virtual, como configurar los dominios de computación, hipervisores e infraestructura de la red.

VM (Virtual Machine): Máquina Virtual. Software que simula a un host y que puede ejecutar programas como si fuese un ordenador real.

VNF (Virtualized Network Function): utiliza las máquinas virtuales que ofrece el bloque NFVI, construyendo sobre ellas las funciones virtualizadas de red añadiendo el software necesario.

VoIP (Voice over IP): Conjunto de normas, dispositivos, protocolos (tecnología) que permite transmitir voz sobre el protocolo IP.

XML (Extensible Markup Language): Lenguaje que permite el almacenamiento y etiquetado de documentos web.

8. Bibliografía

[1] Documento publicado del Reglamento general de protección de datos, publicado en el BOE, y en el diario oficial de la Unión Europea (European Union law) respectivamente, URLs:
https://www.boe.es/doue/2016/119/L00001-00088.pdf
https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX%3A32016R0679

[2] Documento del Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal. URL:
https://www.boe.es/buscar/act.php?id=BOE-A-2008-979

[3] LEY ORGÁNICA 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal. URL:
https://www.boe.es/boe/dias/1999/12/14/pdfs/A43088-43099.pdf

[4] URL de la Comisión Europea con todos los textos legales que afectan a la privacidad y protección de datos, incluyendo directivas derogadas por el GDPR:
https://ec.europa.eu/info/law/law-topic/data-protection/data-protection-eu_en

Web educativa donde pueden verse los puntos clave del Reglamento:
https://www.eugdpr.org

[5] Guías de la Agencia española de protección de datos sobre las relaciones laborales, y otros temas, URL:
https://www.aepd.es/guias/index.html
https://www.aepd.es/media/guias/guia-rgpd-para-responsables-de-tratamiento.pdf
https://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/Guias/GUIA_RelacionesLaborales2.pdf

[6] Web relacionada con servicios de centralitas virtuales de VoIP en nube:
https://www.voip-info.org/cloud-computing
https://www.voip-info.org/what-is-voip y https://www.voip-info.org/cloud-pbx

[7] URL de la ETSI, que explica su gestor de infraestructura virtual (VIM):
https://osm.etsi.org/wikipub/index.php/VIM_emulator

[8] Descripción del protocolo SIP, URL: https://www.ietf.org/rfc/rfc3261.txt
Mecanismo de privacidad para el protocolo SIP, URL:
https://www.ietf.org/rfc/rfc3323.txt

[9] Estándar de la IETF, para incluir localización en SIP, URL:
https://tools.ietf.org/html/rfc6442

[10] Estándar de la IETF, RFC 3986 Uniform Resource Identifier (URI): Generic Syntax. https://www.ietf.org/rfc/rfc3986.txt

[11] Guía de la Comisión Europea para el cumplimiento del Reglamento, URL: https://ec.europa.eu/commission/sites/beta-political/files/data-protection-factsheet-business-7-steps_es.pdf

[12] Glosario de EUR-lex, departamento legal de la UE, URL: http://eur-lex.europa.eu/eli-register/glossary.html

[13] Artículo de opinión sobre la portabilidad de los datos del Article 29 Working Party opinion 242 rev.01, de la CE, URL: http://ec.europa.eu/newsroom/document.cfm?doc_id=44099

[14] Notificaciones de brechas de seguridad en la AEPD, URL: https://sedeagpd.gob.es/sede-electronica-web/vistas/formBrechaSeguridad/procedimientoBrechaSeguridad.jsf#

[15] Estándares de privacidad para la industria de la ISO, URLs:
ISO 29100 **Privacy framework**
https://www.iso.org/standard/45123.html
ISO 29190, **Privacy capability assessment model**
https://www.iso.org/standard/45269.html
ISO 29134 **Guidelines for privacy impact assessment**
https://www.iso.org/standard/62289.html

[16] Publicación especial NIST 800-38G, Recommendation for Block Cipher Modes of Operation: Methods for Format-Preserving Encryption, autor: Morris Dworkin: Fecha: Marzo 2016
https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-38g.pdf

[17] Descripción del protocolo de la IETF TLSv1.2, fecha: Agosto 2008, autores: Dierks & Rescorla, URL: https://tools.ietf.org/html/rfc5246

[18] Web oficial, de Rsyslog (The Rocket-Fast system for log processing), última versión estable 8.35.0, URL: https://www.rsyslog.com

[19] Gestor de vulnerabilidades español, URL: https://www.csirt.es/index.php/es/login

9. Anexos

Anexamos el artículo 4 del RGPD, donde aparecen las definiciones relativas al Reglamento, para hacer más fácil la lectura del mismo a personas no familiarizadas con el Reglamento.

Artículo 4 Definiciones A efectos del presente Reglamento se entenderá por:

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;
3) «limitación del tratamiento»: el marcado de los datos de carácter personal conservados con el fin de limitar su tratamiento en el futuro;
4) «elaboración de perfiles»: 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;
5) «seudonimización»: el tratamiento de datos personales de manera tal que ya no puedan atribuirse a un interesado sin utilizar información adicional, siempre que dicha información adicional figure por separado y esté sujeta a medidas técnicas y organizativas destinadas a garantizar que los datos personales no se atribuyan a una persona física identificada o identificable;
6) «fichero»: todo conjunto estructurado de datos personales, accesibles con arreglo a criterios determinados, ya sea centralizado, descentralizado o repartido de forma funcional o geográfica;
7) «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;
8) «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;
9) «destinatario»: la persona física o jurídica, autoridad pública, servicio u otro organismo al que se comuniquen datos personales, se trate o no de un tercero. No obstante, no se considerarán destinatarios las autoridades públicas que

4.5.2016 L 119/33 Diario Oficial de la Unión Europea ES puedan recibir datos personales en el marco de una investigación concreta de conformidad con el Derecho de la Unión o de los Estados miembros; el tratamiento de tales datos por dichas autoridades públicas será conforme con las normas en materia de protección de datos aplicables a los fines del tratamiento;

10) «tercero»: persona física o jurídica, autoridad pública, servicio u organismo distinto del interesado, del responsable del tratamiento, del encargado del tratamiento y de las personas autorizadas para tratar los datos personales bajo la autoridad directa del responsable o del encargado;

11) «consentimiento del interesado»: toda manifestación de voluntad libre, específica, informada e inequívoca por la que el interesado acepta, ya sea mediante una declaración o una clara acción afirmativa, el tratamiento de datos personales que le conciernen;

12) «violación de la seguridad de los datos personales»: 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;

13) «datos genéticos»: datos personales relativos a las características genéticas heredadas o adquiridas de una persona física que proporcionen una información única sobre la fisiología o la salud de esa persona, obtenidos en particular del análisis de una muestra biológica de tal persona;

14) «datos biométricos»: datos personales obtenidos a partir de un tratamiento técnico específico, relativos a las características físicas, fisiológicas o conductuales de una persona física que permitan o confirmen la identificación única de dicha persona, como imágenes faciales o datos dactiloscópicos;

15) «datos relativos a la salud»: datos personales relativos a la salud física o mental de una persona física, incluida la prestación de servicios de atención sanitaria, que revelen información sobre su estado de salud;

16) «establecimiento principal»: a) en lo que se refiere a un responsable del tratamiento con establecimientos en más de un Estado miembro, el lugar de su administración central en la Unión, salvo que las decisiones sobre los fines y los medios del tratamiento se tomen en otro establecimiento del responsable en la Unión y este último establecimiento tenga el poder de hacer aplicar tales decisiones, en cuyo caso el establecimiento que haya adoptado tales decisiones se considerará establecimiento principal; b) en lo que se refiere a un encargado del tratamiento con establecimientos en más de un Estado miembro, el lugar de su administración central en la Unión o, si careciera de esta, el establecimiento del encargado en la Unión en el que se realicen las principales actividades de tratamiento en el contexto de las actividades de un establecimiento del encargado en la medida en que el encargado esté sujeto a obligaciones específicas con arreglo al presente Reglamento;

17) «representante»: persona física o jurídica establecida en la Unión que, habiendo sido designada por escrito por el responsable o el encargado del tratamiento con arreglo al artículo 27, represente al responsable o
al encargado en lo que respecta a sus respectivas obligaciones en virtud del presente Reglamento;

18) «empresa»: persona física o jurídica dedicada a una actividad económica, independientemente de su forma jurídica, incluidas las sociedades o asociaciones que desempeñen regularmente una actividad económica;

19) «grupo empresarial»: grupo constituido por una empresa que ejerce el control y sus empresas controladas;
20) «normas corporativas vinculantes»: las políticas de protección de datos personales asumidas por un responsable o encargado del tratamiento establecido en el territorio de un Estado miembro para transferencias o un conjunto de transferencias de datos personales a un responsable o encargado en uno o más países terceros, dentro de un grupo empresarial o una unión de empresas dedicadas a una actividad económica conjunta;
21) «autoridad de control»: la autoridad pública independiente establecida por un Estado miembro con arreglo a lo dispuesto en el artículo 51; 4.5.2016 L 119/34 Diario Oficial de la Unión Europea ES
22) «autoridad de control interesada»: la autoridad de control a la que afecta el tratamiento de datos personales debido a que: a) el responsable o el encargado del tratamiento está establecido en el territorio del Estado miembro de esa autoridad de control; b) los interesados que residen en el Estado miembro de esa autoridad de control se ven sustancialmente afectados o es probable que se vean sustancialmente afectados por el tratamiento, o c) se ha presentado una reclamación ante esa autoridad de control;
23) «tratamiento transfronterizo»: a) el tratamiento de datos personales realizado en el contexto de las actividades de establecimientos en más de un Estado miembro de un responsable o un encargado del tratamiento en la Unión, si el responsable o el encargado está establecido en más de un Estado miembro, o b) el tratamiento de datos personales realizado en el contexto de las actividades de un único establecimiento de un responsable o un encargado del tratamiento en la Unión, pero que afecta sustancialmente o es probable que afecte sustancialmente a interesados en más de un Estado miembro;
24) «objeción pertinente y motivada»: la objeción a una propuesta de decisión sobre la existencia o no de infracción del presente Reglamento, o sobre la conformidad con el presente Reglamento de acciones previstas en relación con el responsable o el encargado del tratamiento, que demuestre claramente la importancia de los riesgos que entraña el proyecto de decisión para los derechos y libertades fundamentales de los interesados y, en su caso, para la libre circulación de datos personales dentro de la Unión;
25) «servicio de la sociedad de la información»: todo servicio conforme a la definición del artículo 1, apartado 1, letra b), de la Directiva (UE) 2015/1535 del Parlamento Europeo y del Consejo (1);
26) «organización internacional»: una organización internacional y sus entes subordinados de Derecho internacional público o cualquier otro organismo creado mediante un acuerdo entre dos o más países o en virtud de tal acuerdo.