EUSKO JAURLARITZA GOBIERNO VASCO

AURRERA!

Nº 61

septiembre 2017

Boletín divulgativo de Innovación y Nuevas Tecnologías
Publicado por el Gabinete Tecnológico
Dirección de Informática y Telecomunicaciones

ÍNDICE

Desde 2002, el Gobierno Vasco ha venido desarrollando distintos Planes para impulsar en Euskadi la Sociedad de la Información. A lo largo de los últimos meses, por ejemplo, ha puesto en marcha una serie de ayudas denominadas **PEBA**, cuyo objetivo es acelerar la expansión de la banda ancha en aquellas zonas de Euskadi que por un motivo u otro aun no disponen de ella. A lo largo de este artículo, conoceremos cuál es su origen, sus antecedentes y el papel de la Administración.

El 25 de mayo de 2018 se convertirá en otra fecha importante desde el punto de vista de los derechos de las personas, ya que ese día entrará en vigor el Reglamento 2016/679 del Parlamento Europeo y del Consejo, relativo a la protección de las personas físicas en lo que respecta al **tratamiento de datos personales**. Esta nueva normativa traerá consigo numerosas novedades, por lo que conviene conocer cada una de ellas para ir adaptando nuestra organización y poder así cumplir los nuevos requisitos legales. En el segundo tema de este boletín, por tanto, haremos una primera aproximación a este Reglamento y os presentaremos sus principales características.

En el apartado «*Alboan*», os presentamos un interesante proyecto que han puesto en marcha las Direcciones de Atención a la Ciudadanía, Innovación y Mejora de la Administración (DACIMA) y la de Relaciones Laborales para mejorar el servicio del comedor ubicado en la sede del Gobierno Vasco en Lakua; se trata de un sistema que nos permitirá **tramitar los pedidos del menú del día** sin necesidad de utilizar los tickets en papel que eran imprescindibles hasta ahora. Tras un periodo de pruebas, a partir de ahora las personas que hagan uso del **servicio del comedor** deberán realizar el encargo a través de esta nueva aplicación. Si queréis conocer sus características, no os perdáis el artículo que hemos preparado.

Para acabar, en la sección «Breves», incluiremos una referencia al **acuerdo** que recientemente ha firmado la sociedad informática del Gobierno Vasco, EJIE S.A., con Mondragon Unibertsitatea, donde detallaremos cuál es su objetivo y las acciones que se tienen previsto llevar a cabo dentro del mismo. Y como segundo punto, hablaremos del **robo de datos** personales en internet.

Plan PEBA: Banda Ancha para toda Euskadi

Disponer de unas buenas telecomunicaciones es fundamental para que un país pueda ser cada día más competitivo. Con el objetivo de que todas las regiones de Europa estén en igualdad de condiciones, las Administraciones Públicas están impulsando distintos Planes para extender la Banda Ancha[1], y Euskadi no se queda atrás.

[1] **Banda ancha:** los servicios de acceso de banda ancha son aquellos que permiten a una persona, usando un terminal (ordenador, móvil, etc.) disponer de una conexión a Internet permanente y con una capacidad de transmisión elevada.

Las velocidades se miden por **bits por segundo**, por ejemplo, kilobits por segundo (kbit/s) o megabits por segundo (Mbit/s).

El concepto de banda ancha ha evolucionado a lo largo de los años. La velocidad que proporcionaba, por ejemplo, el RDSI era de 128 Kb/s, después se pasó al ADSL con una velocidad de 256 Kb/s, y actualmente se habla de 25 Mb/s simétricos.

Los servicios de banda ancha suelen comercializarse empaquetados con otros servicios de telecomunicaciones, como el servicio telefónico fijo y/o móvil, así como servicios de televisión.

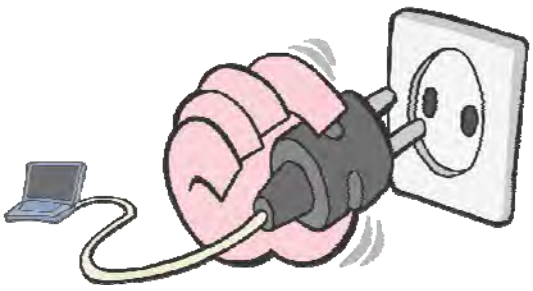
[2] **ISP:** el significado de estas siglas es «*Internet Service Provider*» (en castellano, «*Proveedor de Servicios de Internet*»).

Que una persona o empresa (independientemente de donde resida o donde esté establecida) disponga de una conexión a Internet rápida y segura, se considera hoy en día un elemento clave para una sociedad moderna, ya que ello le permitirá realizar actividades cotidianas o cualquier trámite con la Administración de una manera fácil y cómoda, lo cual irá en aumento debido, entre otras cosas, a la **Ley 39/2015**, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, que pretende impulsar el uso de los medios telemáticos por parte de la ciudadanía.

Sin embargo, y aunque parezca extraño, algunas zonas de nuestro entorno todavía no disponen de una buena conexión a Internet ni de las infraestructuras adecuadas. La principal razón es económica, ya que para una compañía de telecomunicaciones o ISP[2] puede serle muy costoso ofrecer el servicio en esas zonas. Instalar y configurar toda la infraestructura necesaria le puede suponer una gran inversión y el número de clientes potenciales (personas o empresas) es muy reducido, por lo que al ISP puede que no le sea rentable hacer la inversión.

OBJETIVO 2020

Para lograr que todas las personas estén en



Comisión Europea

igualdad de condiciones y dispongan de los mismos recursos, independientemente de su lugar de residencia, a lo largo de los últimos años las Administraciones Públicas han puesto en marcha distintos Planes. En esta ocasión, nos centraremos en el «PEBA», siglas de «Programa de Extensión de la Banda Ancha (PEBA)», cuyo objetivo es precisamente acelerar la implantación de las infraestructuras necesarias para que todas las personas/empresas de una zona determinada dispongan de acceso a la Banda Ancha.

A diferencia de otros Planes anteriores o similares a éste, las ayudas o subvenciones PEBA van destinadas a las empresas operadoras de telecomunicaciones, ya que son ellas quienes se encargarán, en última instancia, de instalar la infraestructura que permitirá ampliar la cobertura de las redes de telecomunicaciones, lo cual impulsará además la sociedad de la información y el conocimiento en cualquier territorio de la Unión Europea.

En definitiva, con esta iniciativa las Administraciones pretenden apoyar a las zonas más remotas y en riesgo de despoblación de cada uno de los países miembros de la Unión Europea, ya que, tal y como se afirma en varios informes de la UE, «*los datos de 2014 indican que los ciudadanos*

y las empresas de la UE se conectan más, compran más por internet, tienen mayor confianza y manejan mejor las tecnologías de la información y las comunicaciones. […] Los datos señalan también que en la UE, especialmente en las zonas rurales, hay mucha gente que no usa la banda ancha de alta velocidad para satisfacer sus necesidades digitales y el déficit de competencias digitales sigue siendo un gran problema.»

Ya en 2010, la Comisión Europea, en la «*Agenda Digital para Europa 2020*» indicaba lo siguiente:

«*Aunque 250 millones de europeos se sirven de internet a diario, aún hay millones que nunca lo han utilizado. Las personas con discapacidad tienen especiales dificultades a la hora de disfrutar de los nuevos contenidos y servicios electrónicos. Cada vez más tareas cotidianas se hacen en línea: para participar plenamente en la sociedad todos necesitamos una mayor capacitación digital.*»

En dicha Agenda Digital, que incluía 101 acciones agrupadas en 7 pilares, uno de los cuales (en concreto, el cuatro) hacía referencia al «*Acceso rápido y ultrarrápido a Internet*», se establecían los siguientes dos grandes objetivos para **2020**:

- ✓ Que toda la población tenga acceso al servicio de Banda Ancha de Nueva Generación (30 Mbps como mínimo).
- ✓ Que al menos el 50% de la población tenga acceso al servicio de Banda Ancha ultrarrápida (velocidad superior a 100 Mbps).

Se considera que alcanzar estos objetivos «*abrirá el camino a servicios innovadores como la sanidad electrónica, las ciudades inteligentes y la economía de los datos.*».

Desde el punto de vista tecnológico se ha optado por potenciar las conexiones de Banda Ancha o NGA[3]. [ver cuadro titulado «*Redes NGA*»]

Sin embargo, y antes de realizar el despliegue tecnológico, se han elaborado distintos

(HFC); las FTTH (del inglés «*Fiber To The Home*», en castellano Fibra óptica hasta el hogar); las radioeléctricas basadas en WiMAX y las redes móviles 3,5G (UMTS con HSPA) y 4G (LTE).

Según el último informe elaborado por la CNMC (Comisión Nacional de los Mercados y la Competencia), titulado «*Análisis Geográfico de los servicios de banda ancha y despliegue de NGA en España*» (publicado en abril de 2017), se estima que a junio de 2016 los accesos instalados de banda ancha de nueva generación han aumentado en España un 29,5%, alcanzando los 37,2 millones.

Redes NGA

La cobertura de **banda ancha básica** a 1 Mbps está disponible desde el 1 de enero de 2012 para cualquier persona que la solicite a Telefónica de España (Movistar), en su calidad de operador designado para la prestación del servicio universal, independientemente de su localización geográfica.

Sin embargo, las Tecnologías siguen avanzando y ahora se trata de extender las redes de acceso de nueva generación o NGA, es decir, son aquellas que permiten velocidades de banda ancha de más de 30 Mb/s.

La tecnología que permite ofrecer ese tipo de servicios de banda ancha engloba las redes ADSL[4] («*Asymmetric Digital Subscriber Line*»; en castellano, Línea de Abonado Digital Asimétrica de abonado digital sobre pares de cobre) y VDSL («*Very high-bit-rate Digital Subscriber Line*», línea de abonado digital de muy alta tasa de transferencia); las de cable, con soluciones híbridas de fibra y coaxial

[3] **NGA:** son las siglas en inglés de «*Next Generation Access networks*», que en castellano se traduciría como Redes de acceso de Nueva Generación.

[4] **ADSL:** si queréis saber más sobre esta tecnología y sus principales características, podéis consultar el artículo titulado «*ADSL*» publicado en el boletín Aurrera nº 3 (marzo de 2001)

estudios sobre cada territorio para conocer cuál es su situación actual y saber qué pasos son necesarios realizar a corto y medio plazo. Para ello, se han tenido en cuenta las infraestructuras de telecomunicaciones que cada zona o localidad tiene actualmente y se han establecido tres categorías:

- **Zona Blanca**: en esta categoría se engloban las zonas o habitantes que no tienen redes de Banda Ancha de nueva generación y, además, es poco probable que dispongan de ella en los próximos 3 años. En el caso de Euskadi, por ejemplo, alrededor de 86.000 personas viven en una de estas zonas, es decir, aproximadamente el 7% de la población.
- **Zona Gris**: en esta zona sólo hay una red de telecomunicaciones (o se prevé que en los próximos 3 años se despliegue una) y no se prevé que otro operador despliegue otra red NGA. En el caso de Euskadi el 23% de la población, aproximadamente, vive en una de estas zonas.
- **Zona Negra**: en esta zona ofrecen sus servicios como mínimo dos empresas de telecomunicaciones (o se prevé que en los próximos 3 años haya dos operadoras). Por lo tanto, se considera que habrá cierta competencia entre ambas. En el caso de Euskadi, se calcula que aproximadamente el 70% de la población vive en una de estas zonas.

EN EUSKADI

Desde 2002 y hasta la fecha, el Gobierno Vasco, por su parte, ha desarrollado distintos Planes para impulsar la Sociedad de la Información. Cada uno de ellos ha puesto el énfasis en diferentes elementos en función de las prioridades de la sociedad y la economía vasca, pero también de la evolución tecnológica del momento. Repasamos a continuación algunos de ellos y sus principales características:

- **Euskadi2000tres**. Se trata de un plan pionero que, sin ser un plan específico de Sociedad de la Información, incorporó por primera vez el fenómeno digital a las políticas del Gobierno Vasco.

«Estas iniciativas tienes como objetivo acelerar la implantación de las infraestructuras necesarias para que todas las personas/empresas dispongan de acceso a la Banda Ancha.»

- **Plan Euskadi en la Sociedad de la Información 2002-2005** (PESI). Estructuró los ámbitos de la Administración, la Empresa y, especialmente, la Ciudadanía, poniendo especial atención en la incorporación de ordenadores con acceso a internet de la mayor parte de los hogares vascos y en la alfabetización de la ciudadanía. Y es aquí cuando surge la iniciativa **KZgunea**[5]. Se pretendía, con ello, poder activar la demanda de servicios digitales que, tanto la administración como las empresas, ya empezaban a desplegar a través de internet.
- **Plan Euskadi en la Sociedad de la Información 2010** (PESI 2.0). Posee un enfoque mucho más finalista, poniendo el foco en el uso que la ciudadanía y las empresas hacían de estas tecnologías. De ahí que se considerara a las TIC como palanca para la innovación empresarial, para la creación de una ciudadana activa e incluso para la difusión de contenidos en la red.
- **Agenda Digital Euskadi 2015** (AD@15). Este plan mantiene la estructura de Administración + Empresa + Ciudadanía + Infraestructuras, poniendo un especial énfasis en la extensión de la Administración electrónica y la modernización de los servicios

[5] **KZgunea**: bajo el amparo del Plan Euskadi en la Sociedad de la Información (PESI) 2002-2005 se pusieron en marcha una serie de acciones, como pueden ser entre otras, «*Konekta Zaitez*», que subvencionó la compra de ordenadores con conexión a Internet o el «*carné de conducir ordenadores*» (más conocidos como IT Txartela).

Pero una de las iniciativas más ambiciosas en cuanto a la integración de la ciudadanía en la Sociedad de la Información fue el **proyecto KZgunea** por el que se crearía una red de telecentros públicos gratuitos para la formación y el uso de las Tecnologías de la Información y la Comunicación (TIC).

http://www.kzgunea.eus

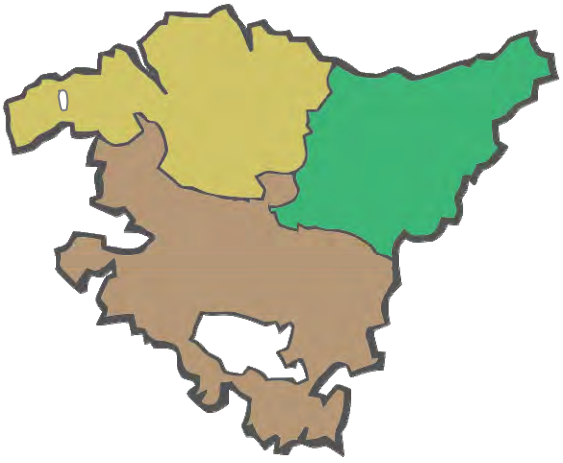
públicos, introduciendo el componente sectorial de estos, como son la sanidad o la educación. También aparecen por primera vez nuevos paradigmas, como el «*Gobierno abierto*».

- **Agenda Digital de Euskadi 2020** (AD@2020). Éste es, precisamente, el Plan del Gobierno Vasco para impulsar la Sociedad de la Información y el Conocimiento en Euskadi, Para ello, se ha estructurado en 4 ejes, 11 retos estratégicos y 62 iniciativas, como pueden ser, entre otras, mejorar la conexión (las telecomunicaciones) de cualquier zona donde viva gente o se ubiquen empresas (polígonos industriales). El objetivo final de esta medida es conseguir un **territorio inteligente y cohesionado**.

Cobertura en el País Vasco (2016)	
Velocidad:	**Cobertura:**
>= 2 Mbps	99%
>= 10 Mbps	96%
>= 30 Mbps	93%
>= 100 Mbps	92%

Fuente: Ministerio de Energía, Turismo y Agenda Digital (MINETAD)

Tal y como se ha indicado al principio, en muchas ocasiones la razón por la que una zona o región no dispone de una buena cobertura se debe a que para las empresas operadoras de telecomunicaciones no les es económicamente rentable ofrecer Banda Ancha. En el caso de Euskadi, por ejemplo, existen más de 800 barrios dentro de las llamadas «Zonas Blancas», la mayoría de las cuales están en Araba y abarcan zonas rurales.



Con objeto de romper o, al menos, disminuir esta «***brecha digital***» y mejorar el «*equilibrio territorial*» entre las zonas bien comunicadas y las que no disponen de la infraestructura necesaria, y cumplir además lo establecido por Europa, se están promoviendo distintos Planes PEBA.

Para ello, el **Gobierno Vasco**, por ejemplo, ha elaborado este año un Plan PEBA (gestionado por el Departamento de Desarrollo Económico e Infraestructuras[6] y cuya dotación económica asciende a más de 8 millones de euros) para dar servicio a los polígonos industriales, y en breve publicará otro Plan PEBA (en este caso, gestionado por la Dirección de Informática y Telecomunicaciones), el cual estará dirigido a dar servicio a distintas zonas o núcleos de población. El importe asignado a este programa de ayudas, que estará en vigor durante los ejercicios 2017, 2018 y 2019, asciende en este caso a 10 millones de euros a repartir entre todas las Zonas Blancas.

En este caso, se ha designado a ITELAZPI[7] como Entidad Colaboradora, es decir, será esta sociedad pública quien se encargue de examinar y evaluar las ofertas que se presenten.

Todas estas iniciativas, en definitiva, tienen como fin último el impulsar la sociedad de la información y el conocimiento, así como de mejorar la calidad de vida y la economía de las personas y territorios de la Unión Europea.

[6] **Departamento de Desarrollo Económico e Infraestructuras**: para más información sobre esta ayuda podéis consulta la Orden de 27 de junio de 2017, de la Consejera de Desarrollo Económico e Infraestructuras, por la que se regula y convoca, para el ejercicio 2017, el programa de ayudas a la extensión de redes de banda ancha de nueva generación en **polígonos empresariales** de Euskadi.

(BOPV nº 130, de 10 de julio de 2017)

[7] **Itelazpi**: es la sociedad pública de telecomunicaciones del Gobierno Vasco (creada en 2003) que gestiona una red terrestre de más de 240 centros, siendo su principal tarea gestionar la red de transporte y difusión de las señales de televisión y radio.

Para más información podéis consultar el boletín Aurrera nº 13 (marzo de 2004)

http://www.itelazpi.eus

Reglamento Europeo de Protección de Datos

A partir del próximo 25 de mayo de 2018 se deberá aplicar el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de sus datos personales.

[8] **AEPD:** Agencia Española de Protección de Datos, es la autoridad pública independiente encargada de velar por la privacidad y la protección de datos de la ciudadanía.

https://www.agpd.es

A partir de mayo de 2018, y debido a las novedades legislativas (sobre todo al nuevo Reglamento Europeo sobre protección de datos personales), nuestra organización va a tener que adaptarse a la nueva legislación, lo que implica revisar su política de protección de datos de carácter personal y de seguridad de la información, y, como no, también sus procesos asociados.

Este nuevo Reglamento General de Protección de Datos (RGPD, en adelante), **se adopta**, no se traspone (es decir, es directamente aplicable, como señalamos más adelante).

Si bien el RGPD entró en vigor el pasado 25 de mayo de 2016, se deberá aplicar al cabo de dos años de su entrada en vigor, es decir, a partir del 25 de mayo de 2018. En estos dos años *los Estados miembros pueden adoptar o iniciar la elaboración de determinadas normas que sean necesarias para permitir o facilitar la aplicación del Reglamento, pero estas normas no pueden ser contrarias a las disposiciones de la vigente Directiva ni tampoco ir más allá de los poderes de actuación normativa que el propio Reglamento prevé de forma explícita o implícita* (fuente AEPD[8]). Esto significa que es directamente aplicable a todos los estados miembro, y que se deberán de eliminar situaciones de incertidumbre derivadas de la existencia de normas nacionales incompatibles con el RGPD (el Reglamento es una norma jurídica con alcance general y eficacia directa).

¿A qué organizaciones se aplica el RGPD? El Reglamento *se aplicará a responsables o encargados de tratamiento de datos establecidos en la Unión Europea, ampliándose a responsables y encargados no establecidos en la UE siempre que realicen tratamientos derivados de una oferta de bienes o servicios destinados a ciudadanos de la Unión o como consecuencia de una monitorización y seguimiento de su comportamiento* (fuente AEPD).

SITUACIÓN ACTUAL

A día de hoy la **política de protección de datos de carácter personal** en el ámbito de la administración pública de la Comunidad Autónoma de Euskadi (que engloba a los Departamentos y Organismos Autónomos) se basa en un Acuerdo de Consejo de Gobierno (ACG) de 16 de julio de 2002, sobre la organización de la seguridad de los ficheros automatizados de datos de carácter personal de la administración de la Comunidad Autónoma del País Vasco. (Expte. Núm.: 20020062A710244).

LOPD Y RMS

Hay que tener en cuenta que en el año 2002

estaban vigentes la Ley Orgánica 15/1999, de 13 de diciembre de Protección de Datos de carácter Personal (LOPD, en adelante) y el Reglamento de Medidas de Seguridad de los ficheros automatizados que contengan datos de carácter personal, aprobado por Real Decreto 994/1999, de 11 de junio (RMS, en adelante); este Reglamento sólo hacía referencia a los ficheros automatizados (en soporte magnético), y no a los ficheros no automatizados (en soporte papel).

RD 1720/2007 Y ROLES ASOCIADOS

Posteriormente, en el año 2007, se publicó el 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, que abarca tanto a ficheros automatizados como a ficheros no automatizados, y deroga el RMS.

Actualmente existen **tres figuras** importantes respecto a la legislación de protección de datos de carácter personal: la persona Responsable o Encargada de Fichero, la entidad responsable de Tratamiento y la persona Responsable de Seguridad. El ACG atribuye una serie de competencias a las personas Responsables de Fichero y a las personas Responsables de Seguridad, asimismo dice que «*todos los ficheros automatizados que contengan datos de carácter personal deberán estar adscritos a una unidad orgánica con rango de Dirección*» (Direcciones Sectoriales como Responsables de Fichero con datos de carácter personal), de modo que sea ésta la que asume la posición de Responsable de Fichero o Tratamiento, y recomienda que la persona Responsable de Seguridad de todos los ficheros con datos de carácter personal de un Departamento sea la misma.

ENCARGADO DE TRATAMIENTO

La Sociedad Pública Eusko Jaurlaritzaren Informatika Elkartea A.B./Sociedad Informática del Gobierno Vasco, S.A. (en adelante EJIE[9]) es la que se ocupa de la prestación de servicios informáticos a la Administración de la Comunidad Autónoma del País Vasco (según la disposición adicional segunda Decreto 35/1997, de 18 de febrero, por el que se regula la planificación, organización, distribución de funciones y modalidades de gestión en materia de sistemas de información y telecomuni-caciones), por lo que actúa como encargado del tratamiento, por cuenta del responsable del fichero (según el ACG «*el responsable del fichero podrá encargar el tratamiento de datos a EJIE, que, como encargado del tratamiento, actuará por cuenta del responsable de éste, de acuerdo con lo estipulado en el contrato-programa que vincula a la mercantil con la Administración de la Comunidad Autónoma del País Vasco (o, en su caso, en el correspondiente convenio) y con las instrucciones dadas por el responsable del fichero*»). No obstante, pueden existir otros encargados de tratamiento distintos a EJIE.

DIRECCIONES SECTORIALES, RF Y RS

Luego tenemos que el ACG marca que los Responsables de Fichero (RF) son las Direcciones Sectoriales, con Responsables de Seguridad (RS) Departamentales (abarcan a un conjunto de Direcciones Sectoriales, las que tenga cada Departamento en su caso), y con al menos un Encargado de Tratamiento, que es EJIE.

RGPD Y RESPONSABILIDAD ACTIVA

El nuevo Reglamento Europeo (RGPD) ante todo es **preventivo**, basándose en lo que se denomina **responsabilidad activa;** para ello contempla una batería de medidas a través

[9] **EJIE:** es la Sociedad Informática del Gobierno Vasco, una empresa pública de servicios de las Tecnologías de la Información y las Comunicaciones (TIC), cuya misión es **contribuir de manera eficaz a la consecución de un Sector Público Vasco moderno y eficiente**, en el Marco Legal establecido por el Gobierno, con la seguridad y calidad establecidas.

de las cuales las organizaciones y empresas aseguran que están en condiciones de cumplir con los derechos, obligaciones y garantías que el propio Reglamento establece. Las medidas son las siguientes:

- ✓ Protección de datos desde el diseño («*privacy by design*»[10])
- ✓ Protección de datos por defecto
- ✓ Medidas de seguridad
- ✓ Mantenimiento de un registro de actividades de tratamientos
- ✓ Realización de evaluaciones de impacto sobre la protección de datos (PIA[11])
- ✓ Nombramiento de una persona que desempeñe el puesto de **delegado de protección de datos (DPD)**
- ✓ Notificación de violaciones de la seguridad de los datos (gestión de incidentes) a la autoridad de control
- ✓ Promoción de códigos de conducta y esquemas de certificación.

RGPD Y ROLES ASOCIADOS

Como hemos señalado en el apartado anterior, aparece una figura nueva, la **persona delegada de protección de datos (DPD)** (desaparece el rol de persona Responsable de Seguridad), junto con las figuras de **responsable de tratamiento** y **encargado del tratamiento**. Cabe destacar que el concepto de *fichero* es sustituido por el de *tratamiento*, y por ende, el anterior responsable de fichero pasa a ser responsable de tratamiento (habrá que establecer la relación entre el fichero con datos de carácter personal actual y las actividades de tratamiento asociadas con este fichero). Asimismo, al no existir ficheros, deja de ser necesario el registro de ficheros con datos de carácter personal, que en nuestro ámbito se realiza ante la Agencia Vasca de Protección de Datos (AVPD[12]), si bien, a partir de mayo de 2018, cada organización deberá llevar un registro de las actividades de tratamiento (el responsable o el encargado del tratamiento debe mantener registros de las actividades de tratamiento bajo su responsabilidad).

RGPD Y ANÁLISIS DE RIESGOS

Para determinar qué medidas aplicar y cómo hacerlo todas las personas responsables de tratamiento deben de realizar **análisis de riesgos de los tratamientos** (utilización sistemática de la información disponible para

Consentimiento según el RGPD

El consentimiento debe darse mediante un acto afirmativo claro que refleje una manifestación de voluntad libre, específica, informada, e inequívoca del interesado/a de aceptar el tratamiento de datos de carácter personal que le conciernen, como una declaración por escrito, inclusive por medios electrónicos, o una declaración verbal. Esto podría incluir marcar una casilla de un sitio web en internet, escoger parámetros técnicos para la utilización de servicios de la sociedad de la información, o cualquier otra declaración o conducta que indique claramente en este contexto que la persona interesada acepta la propuesta de tratamiento de sus datos personales. Por tanto, el silencio, las casillas ya marcadas o la inacción no deben constituir consentimiento. El consentimiento debe darse para todas las actividades de tratamiento realizadas con el mismo o los mismos fines. **Cuando el tratamiento tenga varios fines, debe darse el consentimiento para todos ellos.** Si el consentimiento del interesado/a se ha de dar a raíz de una solicitud por medios electrónicos, la solicitud ha de ser clara, concisa y no perturbar innecesariamente el uso del servicio para el que se presta.

[10] **Privacy by design**: para más información ver el artículo titulado «*Seguridad desde el diseño (privacy by design)*» del boletín Aurrera nº 43 (marzo de 2013)

[11] **PIA**: acrónimo de *Privacy Impact Assessment*, evaluaciones de impacto en la privacidad. Herramienta que permite conocer un producto o servicio desde el punto de vista de la protección de datos personales. Para más información ver boletín Aurrera nº 43 (marzo de 2013).

[12] **AVPD**: Agencia Vasca de Protección de Datos. La Ley 2/2004, de 25 de febrero, de Ficheros de Datos de Carácter Personal de Titularidad Pública y de Creación de la Agencia Vasca de Protección de Datos, configura a ésta como un ente de derecho público, con personalidad jurídica propia y plena capacidad pública y privada, que actúa con plena independencia de las Administraciones Públicas en el ejercicio de sus funciones. www.avpd.euskadi.eus

identificar peligros y estimar los riesgos, en este caso, desde el punto de vista de los tratamientos que contengan datos de carácter personal). Paralelamente, el Esquema Nacional de Seguridad (ENS[13]), dentro de uno de sus principios básicos, artículo 6. *Gestión de la seguridad basada en los riesgos*, también establece el análisis y la gestión de riesgos como aspecto clave en el ámbito de la Administración Electrónica, que tiene la finalidad de poder dar satisfacción al **principio de proporcionalidad** en el cumplimiento de los principios básicos y requisitos mínimos para la protección adecuada de la información. Para realizar esta nueva tarea se puede utilizar una metodología ya conocida, como puede ser MAGERIT[14].

CONSENTIMIENTO DE LA PERSONA INTERESADA: EXPRESO VS TÁCITO

La LOPD exige el consentimiento inequívoco de la persona interesada para el tratamiento de sus datos personales, salvo que nos encontremos bajo algunos de los supuestos que eximen de ese permiso (Administraciones, amparo legal, fuentes accesibles al público, por motivos contractuales…). En cualquier otro caso lo normal es que lo hayamos conseguido durante la recogida de los datos. Este consentimiento estará limitado al tratamiento cuyas finalidades se han incluido en la cláusula de información al interesado/a. Pero ¿qué ocurre si queremos ampliar las finalidades del tratamiento o cederlos? Aquí **el Reglamento que desarrolla la LOPD nos da la posibilidad de obtener el llamado consentimiento tácito** (no dicho formalmente, sino que se supone e infiere); en contraposición a esta norma, para el RGPD una de las bases para tratar los datos personales es el consentimiento, y pide que éste, con carácter general, sea libre, informado, específico e inequívoco, es decir, **el consentimiento no puede deducirse del silencio o de la inacción de la ciudadanía**. Por ello, y a excepción de algunos casos concretos, este consentimiento debe ser explícito. También debe de tener el carácter de revocable (con la misma facilidad que se da para prestarlo), asimismo, es válido el consentimiento dado por una persona menor que tenga 16 años o más.

RGPD Y NUEVAS DEFINICIONES

En el RGPD aparecen nuevas definiciones, entre las cuales podemos destacar las siguientes:

- 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.*
- Tratamientos: cualquier operación u operaciones (automatizadas o no) realizadas sobre los datos personales o conjunto de estos.
- 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.*

RGPD Y NUEVAS CATEGORÍAS Y NUEVOS DERECHOS

El nuevo reglamento Europeo incluye nuevas categorías de datos: **genéticos y biométricos**; asimismo, regula nuevos derechos de la ciudadanía, como son el derecho de supresión, olvido y derecho a la **portabilidad** de los datos de un sistema de tratamiento electrónico a otro. ❑

[13] **ENS**: son las siglas de Esquema Nacional de Seguridad. Para más información consultar el artículo «*Plan de adecuación al Esquema Nacional de Seguridad y al Manual de Seguridad de PLATEA*», publicado en el boletín Aurrera nº 40 (diciembre de 2010).

[14] **MAGERIT**: es la metodología de análisis y gestión de riesgos elaborada por el Consejo Superior de Administración Electrónica que estima que la gestión de los riesgos es una piedra angular en las guías de buen gobierno.

ALBOAN:

Tickets Jantoki Lakua

«Este proyecto pretende proporcionar una mejor experiencia de servicio a las personas clientes del comedor»

El proyecto «**Tickets Jantoki Lakua**», liderado por la Dirección de Atención a la Ciudadanía, Innovación y Mejora de la Administración (DACIMA), junto con la Dirección de Relaciones Laborales (responsable del servicio de comedor en la sede de Lakua), tiene como objetivo final la **digitalización del ciclo de vida de los tickets de comida del comedor de Lakua**, es decir, digitalizar la emisión del ticket, su posterior consumo y, finalmente, su contabilización como ingreso, lo que se traduce en un mejor servicio a las personas usuarias del comedor, la eliminación del dinero metálico, y la automatización de la contabilización de los ingresos.

Se pretenden evitar las siguientes situaciones: las colas para adquirir tickets, el uso de dinero en metálico y su posterior custodia, el mantenimiento de la máquina expendedora, y el arqueo de caja diario que actualmente se realiza.

WALLET (MONEDERO) DE TICKETS

Las personas usuarias dispondrán de un *wallet de tickets* (monedero) en la «*nube*» de EJIE, donde pueden acumular tickets que se compran utilizando mi**pago** (pasarela de pagos de la administración vasca); asimismo, pueden gestionar su monedero utilizando tanto una **aplicación web de escritorio** (disponible en *euskadi.eus,* para ser utilizada a través de un navegador web), como una **app móvil** que se puede instalar en dispositivos con sistemas operativos *Android* e *iOS*. Gracias a ello la persona usuaria puede:

- Consultar información general sobre el servicio y sobre los menús.
- Adquirir tickets que se podrán presentar en el comedor.
- Consultar el histórico de compra de tickets y el histórico de consumo (utilización) de tickets.

PRESENTACIÓN DE TICKETS EN EL COMEDOR

La persona usuaria del sistema puede hacer uso de uno o varios tickets de su *wallet* (monedero) personal de dos formas:

- Utilizando la aplicación web de escritorio (en el ordenador personal selecciona los tickets a imprimir, los imprime y recorta)

- Utilizando la app móvil instalada en su dispositivo móvil. Basta con que la persona usuaria seleccione el tipo de ticket que quiere utilizar y este aparecerá en la pantalla del dispositivo móvil (no es necesario ni viable imprimir el ticket, este se

presentará a través de la pantalla del dispositivo móvil).

LECTURA DE TICKETS

El personal del servicio de comedor dispone de unos dispositivos de lectura de tickets que escanean el código del ticket (QRCode) y lo validan. Las personas del servicio de comedor, a través del dispositivo de lectura de tickets, pueden ver los tickets leídos.

También, al estar estos dispositivos de lectura permanentemente conectados y sincronizados con el sistema central, detectan si el ticket ya ha sido utilizado (en cuyo caso no puede volver a utilizarse); en caso de que no hubiese conexión con el sistema central, dichos dispositivos pueden operar de forma autónoma, puesto que tienen una réplica de todos los tickets en una base de datos interna (funcionamiento en modo contingencia).

Una vez leído el ticket por el personal del comedor (consumido), este será cancelado en la base de datos central, y cuando se vuelva a consultar por parte de la persona usuaria del servicio de comedor, este ticket ya no estará disponible en su histórico de compras (sí en el de consumos).

APLICACIÓN INTERNA DE GESTIÓN

A través de esta aplicación las personas responsables del servicio de comedor pueden:

- ✓ Gestionar la información del menú diario
- ✓ Obtener información estadística agregada del uso de tickets (optimiza el servicio)
- ✓ Gestionar la contabilización de los tickets

ASPECTOS TÉCNICOS

Todo lo anterior se basa en un complejo núcleo instalado en la «*nube*» de EJIE y que:

- Proporciona servicios Web a las interfaces de usuario (Web pública, app móvil y gestión interna) y a los dispositivos de lectura de código de barras.
- Encapsula la lógica del negocio e interactúa con otros sistemas externos (mi**pago**: pasarela de pagos, Sistema Integral de Pagos y Cobros de la Administración —SIPCA—; plataformas de correo; mensajería…)

La **seguridad** del *wallet* (monedero) es un aspecto clave del sistema de manera que el acceso al mismo estará controlado por:

- ➢ El sistema de seguridad corporativo XLNets (infraestructura de autenticación y seguridad común para todas las aplicaciones o iniciativas del Gobierno Vasco) en la aplicación Web.
- ➢ Un sistema criptográfico de clave pública/privada en el caso de la aplicación móvil, que impide el acceso al monedero desde cualquier otro dispositivo que no sea aquel en el que se instaló la aplicación (remarcar que todas las transmisiones de información utilizan el protocolo seguro HTTPS).

Otras características técnicas:

- Disponible tanto en euskera como en castellano.
- La app móvil es una aplicación nativa de cada plataforma (Android e iOS).
- Permite personas usuarias sin identificador XLNets. ❑

«Permite automatizar la contabilidad, hasta ahora manual, de los ingresos»

¡¡BREVES!!

Nº 61

septiembre 2017

Acuerdo entre EJIE y Mondragon Unibertsitatea

La Sociedad Informática del Gobierno Vasco (EJIE) y Mondragon Unibertsitatea (MU) acaban de firmar un acuerdo para impulsar el desarrollo de talento y proyectos relacionados con las tecnologías de la información y las comunicaciones (TIC).

Mediante este acuerdo ambas entidades se comprometen a «*compartir conocimiento y desarrollar talento en el nuevo paradigma digital*», siendo los objetivos del mismo los siguientes:

- ✓ Promover la colaboración en ámbitos tecnológicos y no tecnológicos fomentando la generación, el **intercambio** y la transferencia de conocimiento.
- ✓ Puesta en marcha actuaciones y programas para la gestión del talento en el mundo digital.

Para ello, el convenio fomentará acciones como:

- Actividades de formación y gestión del talento, tanto en el ámbito profesional como en el universitario.
- Desarrollo de proyectos de investigación cooperativa.
- Realización de **tesis doctorales** conjuntas, co-dirigidas por personal de EJIE y de Mondragon Unibertsitatea.
- Colaboración de profesionales de EJIE en actividades de **formación** en Mondragon Unibertsitatea.
- Participación de estudiantes de Mondragon Unibertsitatea en Trabajos Fin de Máster, Fin de Grado o en prácticas en EJIE.
- Puesta en marcha de proyectos conjuntos con empresas, tanto de investigación como de transferencia de conocimiento.

En definitiva se trata de mejorar la **eficiencia y competitividad** de ambas entidades, abordando la transferencia de talento Universidad-Empresa.

https://www.ejie.eus
http://www.mondragon.edu

Robo de datos en internet

El robo de datos personales en Internet es hoy en día uno de los grandes problemas que podemos sufrir en Internet. El último ejemplo lo tenemos con el robo que ha sufrido Equifax, la entidad que monitoriza el historial crediticio de millones de personas de los Estados Unidos, se ha convertido en el mayor de la historia. **Se calcula que el número de personas afectadas puede superar los 140 millones**. Esto ha sido posible porque un equipo de ciberatacantes ha explotado una vulnerabilidad en el sitio Web de esta compañía del sector financiero.

Aunque la compañía Yahoo! sufrió, a través de dos ataques seguidos, el robo de datos de 1.500 millones de personas usuarias, el sufrido por Equifax es de mayor calado, no por el volumen de personas afectadas, sino por la calidad de los datos robados: no solo contraseñas o tarjetas de crédito, sino que también se incluyen tanto números de la seguridad social como números de permisos de conducir; estos números son equivalentes al documento nacional de identidad (DNI) que utilizamos nosotros, por lo que la mayor amenaza que se cierne sobre las personas de las que se ha conseguido dicha información es la **suplantación de identidad**. Por ello, algunos analistas de seguridad citan a este robo de datos como el peor incidente de la historia. Los datos robados no proviene únicamente de personas de los Estados Unidos, sino que también hay personas clientes de Canadá y del Reino Unido.

Si bien el ciberataque se descubrió el pasado 29 de julio, se ha hecho público a principios del mes de septiembre.

Para las personas que puedan verse afectadas se recomienda suscribir un seguro contra el robo de identidad, estar muy atentos a sus movimientos financieros, y **activar la autenticación en dos pasos** (algo que se tiene, por ejemplo el dispositivo móvil o un *token*, más algo que se sabe); aun así las consecuencias de este robo podrían tener repercusión a largo plazo.