EUSKO JAURLARITZA GOBIERNO VASCO

AURRERA!

Nº 69

septiembre 2019

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

ÍNDICE

- La migración de los teléfonos móviles corporativos Pág. 2
- RAT: el Registro de Actividades de Tratamiento Pág. 6

Alboan:

- Consejos sobre Windows10 y Office365: compartir, coedición y control de versiones Pág. 10

Contraportada:

- Las mujeres y la ciberseguridad
- Ikerbasque premia la labor de las mujeres científicas Pág. 12

Durante los últimos meses, el Gobierno Vasco ha llevado a cabo la migración de los teléfonos móviles de todo su personal, lo que ha supuesto sustituir alrededor de 1.300 terminales. Dadas las novedades que ha traído consigo este proceso, principalmente para garantizar la seguridad y privacidad de los datos de las personas usuarias, hemos dedicado el primer tema a explicar cuáles son esas mejoras. No os perdáis el artículo *«La migración de los teléfonos móviles corporativos»*.

El nuevo Reglamento General de Protección de Datos, que ya está en vigor, ha traído consigo varias novedades que las empresas y/o entidades tienen que implantar en su organización. Una de las más significativas es que ya no es necesario inscribir los ficheros en la Agencia de Protección de Datos correspondiente. Sin embargo, sí establece una nueva obligación, y es que el/la Responsable de Tratamiento debe implantar el Registro de Actividades de Tratamiento. En el segundo tema, titulado *«RAT: el Registro de Actividades de Tratamiento»*, analizaremos qué implica dicho registro y cómo se está abordando esta tarea en el ámbito del Gobierno Vasco.

Dado que la migración a Windows10 y el despliegue del nuevo paquete ofimático Office365 continúa, en el apartado Alboan, os damos una serie de *«Consejos sobre Windows10 y Office365»* que esperamos os sean de utilidad. En este caso, nos centramos en las distintas opciones que hay a la hora de compartir un documento, las características de la coedición a la hora de redactar un documento con la colaboración de otra persona, así como la gestión automática que hace la nueva plataforma del control de versiones de un documento.

Con el artículo *«Las mujeres y la ciberseguridad»* analizamos la situación de la mujer en un sector tradicionalmente masculino, tomando como base un reciente estudio de la asociación «(ISC)²».

Y, para acabar, nos hacemos eco de los premios que por primera vez ha otorgado la fundación Ikerbasque, los cuales tienen como objetivo dar visibilidad a las carreras de mujeres investigadoras brillantes y reconocer su aportación a la ciencia. En el artículo *«Ikerbasque premia la labor de las mujeres científicas»* os damos a conocer el nombre de las 7 científicas vascas que han sido galardonadas.

La migración de los teléfonos móviles corporativos

La migración de los teléfonos móviles corporativos llevada a cabo este año ha sido mucho más que un simple cambio de terminales, ya que los nuevos dispositivos incluyen, además de las novedades propias que ofrecen los nuevos aparatos, la gestión de los mismos para mejorar la seguridad de los datos que almacenan.

Durante los meses de mayo y junio de este año se ha llevado a cabo la migración de los teléfonos móviles del Gobierno Vasco, lo cual ha supuesto sustituir alrededor de 1.300 terminales, y si tenemos en cuenta al resto de entes englobados en el proyecto (Osakidetza, EiTB, SPRI, IHOBE, EVE, HAZI, OSATEK, ETS, UPV/EHU, VISESA… hasta un total de 32 entidades) el volumen de líneas migradas supera las 10.000.

EL CONTRATO

El nuevo contrato de comunicaciones del Gobierno Vasco[1], que tiene una duración de 2 años (con opción de prórroga), ha sido adjudicado finalmente a la empresa Vodafone, que sustituye a la anterior adjudicataria, Telefónica/ Movistar.

En cuanto a los terminales que ha ofrecido Vodafone al Gobierno Vasco, se han establecido tres categorías: Altos Cargos, Personal Técnico y Personal Técnico con necesidades especiales.

[ver tabla *«Relación de teléfonos móviles y perfil de las personas usuarias»*]

El catálogo completo de terminales y sus características principales se puede consultar en Jakina[2]. A parte de los teléfonos móviles, algunas personas usuarias, en función de sus necesidades, tendrán también a su disposición

Relación de teléfonos móviles y perfil de las personas usuarias

Perfil del usuario/a	Gama	Móviles
Altos Cargos	Phablet	iPhone XS Max Samsung S10+ Nokia 9 Pure View Galaxy Note 9
	Smartphone	iPhone XS Samsung S10E Nokia 8 Sirocco
Personal Técnico *(con necesidades especiales)*	Especial	Samsung A50 EE Samsung S9 BQ Aquaris X2
Personal Técnico	Normal	Samsung A40 EE Nokia 7.1

[1] **Contrato de comunicaciones:** el nuevo contrato se basa en el expediente nº 086-2018 de EJIE, titulado *«Contratación de Servicios de Telecomunicaciones de Telefonía Fija, comunicaciones móviles, SMS Masivo e Internet»* al que se presentaron un total de 4 empresas.

EJIE, a través del Área de Desarrollo de Negocio, se ha encargado de analizar las ofertas recibidas y de adjudicar el expediente. De cara a futuro, será también EJIE quien se encargue de analizar el estado del arte de las soluciones tecnológicas existentes en el mercado, los factores de riesgo, realizar pruebas, etc.

[2] **Catálogo de terminales:** el nuevo catálogo de terminales homologados y demás información relacionada con la migración (manuales, guías, etc.), se puede consultar en la Intranet del Gobierno:

«Jakina

+ Trabajo

+ Informática y telecomunicaciones

+ Telefonía - Comunicaciones RCA»

un nuevo aparato que recibe el nombre de MiFi.

[ver cuadro *«Un nuevo dispositivo llamado MiFi»*]

Una de las principales características de este expediente de contratación es que va a ser la Sociedad Informática del Gobierno Vasco, **EJIE**, la encargada de gestionarlo, aunque será cada entidad la que decida después cómo realizar el *«onboarding»* o la implantación de ese servicio (A día de hoy, «Comunicaciones móviles» se ha implementado ya como un servicio más dentro del Catálogo de Servicios de EJIE, para que puedan hacer uso de él todas las entidades que así lo deseen).

Por otro lado, es importante destacar que los nuevos móviles vienen ya configurados de tal forma que, por defecto, se conecten a la red WiFi Corporativa del Gobierno Vasco (identificada con el SSID *«Batera_mobile»*). De esta forma, cuando tengamos una antena WiFi de esta red al alcance, el tráfico saldrá por esa antena y, gracias a ello, se conseguirá reducir la factura de datos del teléfono móvil (ya que el nuevo contrato, al igual que el anterior, se factura por consumo, pero sin franquicias de tráfico).

«El personal técnico de EJIE gestionará y controlará la seguridad de los nuevos terminales, sin tener acceso en ningún caso a la información personal o aplicaciones que pueda manejar el usuario/a final»

UN NUEVO DISPOSITIVO LLAMADO MiFi

Hasta ahora, cuando una persona necesitaba tener conexión a Internet (o acceder vía VPN a la Red Corporativa del Gobierno Vasco), lo habitual era entregarle un **módem USB** que debía conectarse y configurar a su ordenador portátil.

A partir de ahora, sin embargo, no se van a entregar módems USB, y en su lugar las personas usuarias que necesiten conectarse a Internet deberán usar la opción que ofrecen los propios teléfonos móviles, y que consiste en **compartir su conexión de internet**. Para ello, la misma persona usuaria únicamente deberá activar esa opción en su propio móvil cada vez que lo necesite: «Ajustes» + «Conexiones» + «Compartir conexión» [los nombres de estas opciones pueden variar en función del teléfono que tengamos].

Sólo en aquellos casos en los que se estime que se va a hacer un uso intensivo de Internet, y que la persona usuaria puede quedarse sin datos en el móvil, la DIT entregará un dispositivo llamado **MiFi**[3], que hace las funciones del antiguo módem USB y que su configuración y uso es mucho más sencillo. Por lo tanto, los módems USB que se estaban usando hasta la fecha, ya no estarán operativos y deberán entregarse a la DIT para ser devueltos a Telefónica.

¡Importante!

A la hora de usar un MiFi, es aconsejable primero **eliminar el PIN** de la tarjeta que lleva asociada.

Para ello, la persona usuaria final deberá insertar esa tarjeta en un teléfono móvil, o en un dispositivo que gestione tarjetas SIM, por ejemplo, e ir a «Ajustes» y seleccionar/desactivar la opción correspondiente (que variará en función del teléfono que tengamos) para que no nos solicite el PIN. Una vez hecho eso, la persona usuaria introducirá la tarjeta en el MiFi, lo encenderá y listo para ser utilizado.

Ahora ya podremos usar ese MiFi sin ningún problema.

[3] **MiFi:** es el nombre comercial creado por la empresa Novatel Wireless usado para referirse a un *router* inalámbrico que actúa como *hotspot wifi* móvil.

Un MiFi es un dispositivo que puede conectarse a una red móvil y gracias a ello proporciona acceso a internet a varios dispositivos simultáneamente.

El primer MiFi fue lanzado en Estados Unidos en mayo de 2009 por Novatel Wireless.

Aunque la empresa nunca se ha pronunciado al respecto, se cree que la palabra *«MiFi»* hace referencia a *«Mi WiFi»*.

[fuente: https://es.wikipedia.org/wiki/MiFi]

Otra de las grandes novedades que conviene tener en cuenta es que a partir de ahora todas las incidencias relacionadas con los teléfonos móviles (incluidos robos y pérdidas en 24x7) se van a centralizar en el **teléfono 440**, el mismo CAU[4] (Centro de Atención a las Personas Usuarias) que se encarga actualmente de las incidencias informáticas de los ordenadores de la Red Corporativa del Gobierno Vasco.

Con este nuevo contrato el Gobierno Vasco pretende crear un nuevo *«ecosistema»* en el que estén englobados todos los nuevos terminales y alinear esta nueva migración con el proyecto de **convergencia tecnológica**, llamado **Batera**, que está llevando a cabo el Gobierno Vasco y que, entre otras cosas, va a permitir ahorrar costes a todos los entes que participan en el proyecto, así como obtener un valor añadido en todos los servicios implantados.

LA SEGURIDAD

Dado que hasta ahora los terminales móviles que tenía el personal del Gobierno Vasco (tanto técnicos como Altos Cargos) no estaban gestionados de forma centralizada ni estaban securizados, se ha

SEGURIDAD
SANDBLAST MOBILE

Uno de los aspectos más importantes que hoy en día debe cuidar cualquier empresa es la **seguridad** de su red. Teniendo en cuenta que cada vez hay más amenazas y que los teléfonos móviles son los nuevos «vectores de ataque» que usan muchos/as hackers, es imprescindible mejorar el control y protección de esos cada vez más potentes teléfonos.

En muchas ocasiones, los dispositivos móviles son la puerta trasera a través de los cuáles se puede acceder de forma fraudulenta a la red de una empresa, y pueden exponer al riesgo los datos corporativos (información confidencial, etc.). Con objeto de evitar o reducir esos peligros, el Gobierno Vasco ha optado por gestionar los nuevos dispositivos móviles con el software SandBlast Mobile de la empresa CheckPoint.

Esta utilidad, instalada por defecto en los dispositivos de todo el personal del Gobierno Vasco (tanto técnico como Altos Cargos), **encripta la información** y asegura nuestro tráfico en caso de que nos conectemos a una red WiFi que presenta signos de intentar interceptar nuestro tráfico. Gracias a ello permite, entre otras cosas, protegernos de aplicaciones infectadas, ataques del tipo *Man-in-the-Middle* que podamos sufrir a través de redes WiFi, de *exploits* del Sistema Operativo, de *malware* de día cero o de enlaces maliciosos recibidos vía SMS.

Otra de las mejoras que ofrece la plataforma que utiliza EJIE para gestionar los teléfonos móviles es que en el caso de que nos roben el móvil, se puede **proceder de forma remota al bloqueo y borrado de los datos** (personales o confidenciales) que tenga el teléfono y, de esta forma, evitar que caigan en manos no deseadas.

[4] **CAU:** el servicio o Centro de Atención a personas Usuarias está disponible en el siguiente teléfono, 440 (o llamando a los siguientes teléfonos para los centros NO integrados en la Red Corporativa de voz:
- Lakua 945.016.440
- Bizkaia 944.032.440
- Gipuzkoa 943.022.440
- Araba 945.016.440)

O bien a través del buzón de correo electrónico identificado como *«CAU Lakua»*, que tiene asociada la siguiente cuenta de email: cau-ejie@ejie.eus

querido aprovechar esta migración para mejorar la **seguridad** de los terminales y de la información (datos) que puedan albergar. Para ello, todos los terminales móviles quedan ya incluidos dentro de una gestión global corporativa y con un grado de seguridad calificado como alto. Pero para ello, primero es imprescindible proceder al *«enrolamiento»* del teléfono.

«Se tiene previsto realizar auditorías periódicas del "ecosistema" y de la gestión que realiza EJIE»

EL ENROLAMIENTO

El enrolamiento es un proceso que la persona usuaria final debe realizar antes de poder usar el teléfono móvil y su objetivo es simplemente **registrar o inscribir** el nuevo dispositivo en la plataforma de gestión de EJIE, y que va a permitir al personal técnico de EJIE gestionar el teléfono móvil e instalar todas las aplicaciones necesarias para mejorar su seguridad.

Dado que la seguridad es una pieza fundamental en el nuevo entorno que se ha implantado, se tiene previsto realizar **auditorías periódicas** del ecosistema y de la gestión que realiza EJIE. Tal es así que, recientemente, se ha realizado ya la primera de ellas, cuyos resultados finales se darán a conocer en octubre.

APLICACIONES

Gracias al nuevo ecosistema que se ha definido, implantado sobre una plataforma EMM[5], se pueden instalar en el teléfono (también se suele usar el término *push* [«empujar», en inglés]), aquellas aplicaciones corporativas o públicas que se consideren necesarias y que hayan sido validadas o autorizadas por cada entidad responsable de esos terminales (Gobierno Vasco, Osakidetza…). Veamos cuáles se están instalando actualmente:

- El software EMM (en nuestro caso, VMware Intelligent Hub), es el que a su vez permite, por ejemplo, instalar otras aplicaciones, denegar su instalación ante posibles agujeros de seguridad, etc.
- La aplicación SandBlast del fabricante CheckPoint, que mejora la seguridad del teléfono. En este caso, el usuario/a deberá autorizar previamente la ejecución de la aplicación, tal y como se ha establecido en el manual de requerimiento acordado entre el Gobierno Vasco y EJIE. [ver cuadro *«Seguridad SandBlast Mobile»*]

- Varias aplicaciones del paquete ofimático Office365, el entorno colaborativo Teams, y la aplicación de correo electrónico.
- Otras aplicaciones, como puede ser el traductor de euskera Itzultzaile, desarrollado por el propio Gobierno Vasco.

Para ver la lista completa de aplicaciones instaladas en nuestro móvil, podemos pulsar el botón *«App Catalog»* que aparece en nuestro teléfono. A día de hoy, esta lista incluye un total de 14 aplicaciones. Aunque, la idea es que vaya ampliándose con el paso del tiempo. ❑

[5] **EMM:** son las siglas en inglés de *«Enterprise Mobility Management»*, (Administración de movilidad empresarial, en castellano). Se trata de la plataforma que facilita la gestión de todos los dispositivos que van a entrar en nuestros sistemas (red), garantizando la seguridad de toda la red.

En definitiva, permite al personal técnico de EJIE gestionar y controlar la seguridad de los nuevos terminales (sin tener acceso en ningún caso a la **información personal o aplicaciones** que pueda manejar el usuario/a final, garantizando en todo momento la **privacidad y confidencialidad** de sus datos personales, incluyendo sus cuentas de correo y llamadas).

Para más información, podéis consultar el artículo *«Movilidad en la empresa»*, publicado en el boletín Aurrera nº 44, en junio de 2013.

RAT: el Registro de Actividades de Tratamiento

El nuevo Reglamento General de Protección de Datos ha traído consigo varias novedades que las organizaciones tienen que implantar. Una de ellas es que el/la Responsable de Tratamiento debe implantar el Registro de Actividades de Tratamiento. Veamos cómo se está abordando esta tarea en el ámbito del Gobierno Vasco.

Mediante el Decreto 81/2018, de 22 de mayo, de modificación del Decreto por el que se establece la estructura orgánica y funcional del Departamento de Gobernanza Pública y Autogobierno, se crea el órgano de la Delegada de protección de datos de la Comunidad Autónoma de Euskadi. Está adscrito a la Viceconsejería de Régimen Jurídico del Departamento de Gobernanza y Autogobierno, pero sin integrarse en su estructura jerárquica, ejerciendo sus funciones con plena autonomía jerárquica y funcional.

Entre las funciones principales de la Delegada de protección de datos se destacan las siguientes:

- **Coordinar y apoyar** a los órganos responsables del sistema de información pública designados por los departamentos, los organismos autónomos y los entes públicos de derecho privado (EPDP) de la Comunidad Autónoma de Euskadi.
- **Informar y asesorar** de las obligaciones que les incumben, a:
  - ✓Responsables de tratamiento
  - ✓Encargado de tratamiento
  - ✓Responsables de las medidas de privacidad
  - ✓Referentes de protección de datos
- **Supervisar** el cumplimiento del Reglamento General de Protección de Datos (RGPD[6]), de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, y de las políticas del responsable o del encargado del tratamiento en materia de protección de datos personales, incluida la asignación de responsabilidades, la concienciación y formación del personal que participa en las operaciones de tratamiento, y las auditorías correspondientes.
- **Ofrecer el asesoramiento** que se le solicite acerca de la evaluación de impacto relativa a la protección de datos y supervisar su aplicación
- **Cooperar** con la Agencia Vasca de Protección de Datos[7]
- **Actuar como punto de contacto** de la Agencia Vasca de Protección de Datos para cuestiones relativas al tratamiento, incluida la consulta previa a que se refiere el artículo 36 del RGPD, y realizar consultas, en su caso, sobre cualquier otro asunto

«El RGPD establece la obligación de crear y mantener un registro de las actividades de tratamiento efectuadas»

La Delegada de protección de datos desempeña sus funciones prestando la debida atención a los riesgos asociados a las operaciones de tratamiento, teniendo en cuenta la naturaleza, el alcance, el contexto y fines del tratamiento.

Para la gestión de las tareas propias de la protección de los datos personales en la Administración Pública Vasca, mediante Acuerdo de Gobierno de 18 de junio de 2018, se aprobó la estructura organizativa y la asignación de los «roles» para la protección

[6] **RGPD:** Para conocer las gestiones realizadas por parte del Gobierno Vasco durante los últimos meses para adecuarse a la nueva normativa, podéis consultar los siguientes documentos:

- Artículo *«Adecuación del Gobierno Vasco al RGPD»* publicado en el boletín Aurrera número 67 (marzo 2019)
- Artículo *«Adecuación al nuevo Reglamento de Protección de Datos»* publicado en el boletín Aurrera número 65 (septiembre 2018)

[7] **AVPD:** Página web de la Agencia Vasca de Protección de Datos. www.avpd.euskadi.eus

de los datos personales tratados por la Administración Pública de la Comunidad Autónoma de Euskadi. Este acuerdo afecta a todos los Departamentos de la Administración Publica de la Comunidad Autónoma de Euskadi, sus Organismos Autónomos y Entes Públicos de Derecho Privado.

ROLES

Los roles en la protección de datos personales en la Administración Pública de la CAE[8] son los siguientes:

Responsable de Tratamiento (RT)

Lo ejerce la persona titular del respectivo órgano del Departamento, o del órgano unipersonal de gobierno correspondiente a cada Organismo Autónomo o Ente Público de Derecho Privado.

Encargado de Tratamiento (ET)

Es la persona física o jurídica, autoridad pública, servicio u otro organismo que trate datos personales por cuenta del responsable del tratamiento. El tratamiento de los datos personales por el Encargado de tratamiento

se regirá por un contrato u otro acto jurídico en virtud de lo establecido en la normativa en vigor, que vincule al Encargado respecto del Responsable del tratamiento, y que establezca el objeto, la duración, la naturaleza y finalidad del tratamiento, el tipo de datos personales y categorías de interesados, y la asignación de obligaciones y derechos con respecto al tratamiento de datos personales del responsable.

Responsable de las medidas de Privacidad (RP)

El rol de Responsable de las medidas de privacidad de cada Departamento de la Administración General lo ejerce la persona titular de la **Dirección de Servicios** u órgano equivalente del Departamento respectivo. En los Organismos Autónomos o Entes Públicos de Derecho Privado, el rol de Responsable de las medidas de privacidad lo ejerce la persona titular del órgano unipersonal de gobierno correspondiente a cada Organismo Autónomo o Ente Público de Derecho Privado o la persona que designe dentro de su organización.

Referente (R)

La labor de las personas que ejerzan el cargo de Referentes de protección de datos será la de asistir a la Delegada de protección de datos en el ámbito de la actividad de su Departamento, Organismo Autónomo o Ente Público de Derecho Privado al que pertenezcan. Habrán sido nombrados formalmente por la persona responsable de las medidas de privacidad de su organización.

Asimismo, estos nombramientos deberán notificarse a la Delegada de protección de datos.

TRANSICIÓN DE FICHEROS A TRATAMIENTOS DE DATOS PERSONALES

La anterior legislación en materia de protección de datos establecía la obligatoriedad de declarar y notificar a la Agencia Vasca de Protección de Datos los ficheros que contenían datos personales para su inscripción en el Registro General de Protección de Datos. Esta operación se realizaba mediante Ordenes del Consejero o Consejera y debían ser publicadas en el B.O.P.V. Con el Reglamento General de Protección de Datos (RGPD) desaparece dicha obligación.

El RGPD (artículo 30) establece como una de las novedades más importantes la obligación de los responsables de tratamiento y encargados de tratamiento de datos de **creación y mantenimiento de un registro de las actividades de tratamiento**

[8] **Normativa:** podéis consultar la normativa en vigor en la CAE sobre protección de datos en la siguiente web:
https://www.euskadi.eus/normativa-proteccion-de-datos-personales/web01-a2datuba/es/

efectuadas bajo su responsabilidad. El artículo 30.1 dicta su contenido para el responsable de tratamiento, y el 30.2 para el encargado de tratamiento cuyo detalle es de menor intensidad.

Se trata de un registro de tratamientos, no de ficheros, entendiendo el RGPD por 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.

La finalidad de este registro se basa en el principio de **responsabilidad proactiva**, uno de los principios fundamentales del RGPD, cuyo fundamento es que no solo hay que cumplir la norma sino también poder demostrar su cumplimiento. Es una herramienta que permite tener una perspectiva general de todas las actividades de tratamiento que la organización está llevando a cabo. Dicho registro está a disposición de la Agencia Vasca de Protección de Datos cuando así lo solicite como autoridad de control. Es, por tanto, un requisito necesario de cumplimiento normativo y además una medida de rendición de cuentas, que es otra de las bases fundamentales de la actual normativa de protección de datos.

La LPDGDD[9] establece, además, que las Administraciones Públicas están obligadas a hacer público el **inventario** y que debe ser accesible por medios electrónicos en la página web de la organización. Constituye, por tanto, una importante medida de **transparencia**.

En resumen: el Registro de Actividades de Tratamiento (RAT[10]) es:

- ✓ Una nueva obligación para las Administraciones Públicas.
- ✓ Una lista resumida que informa de los tratamientos de cada organización.
- ✓ Una lista pública a disposición de la ciudadanía y de la AVPD.

REGISTRO DE ACTIVIDADES DE TRATAMIENTO EN LA ADMINISTRACIÓN PÚBLICA DE LA CAE

Para elaborar este registro y poder trabajar en equipo con las personas referentes en protección de datos, se ha creado desde la oficina de la Delegada de protección de datos un entorno colaborativo *Sharepoint* en el cual se proporciona toda la documentación necesaria en la materia y se establecen unos criterios para su elaboración.

En una primera fase, y con la finalidad de recabar la información que permitiera determinar los tratamientos existentes, así como su grado de cumplimiento del RGPD, se

Tabla 1: Información contenida en el RAT, para Responsable de Tratamiento (RT) y Encargado de tratamiento (ET)

Descripción de la información a recoger	RT	ET
Denominación del tratamiento	✓	✓
Datos del responsable de tratamiento	✓	✓
Datos del encargado de tratamiento		✓
Datos la Delegada de protección de datos	✓	✓
Finalidad del tratamiento	✓	
Categorías del tratamiento		✓
Categorías de interesados	✓	
Categorías de datos personales	✓	
Categorías de destinatarios	✓	
Transferencias internacionales (indicando los países a los que se transfieren los datos)	✓	✓
Plazo de conservación	✓	
Medidas de seguridad	✓	✓

[9] **LPDGDD**: se corresponden con las siglas de Ley de Protección de Datos Personales y garantía de los derechos digitales

La Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, regula todo lo relativo a la temática de protección de datos a través del Reglamento Europeo de Protección de Datos, sustituyendo ya, por tanto, y prácticamente de forma completa, a la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal vigente hasta ahora.

Publicada en el BOE nº 294, de 6 de diciembre de 2018.

https://boe.es/diario_boe/txt.php?id=BOE-A-2018-16673

[10] **Registro de Actividades de Tratamiento**: en el caso de la Comunidad Autónoma de Euskadi, el Registro se puede consultar accediendo a la siguiente dirección:

https://www.euskadi.eus/registro-de-actividades-de-tratamiento-rat/web01-a2datuba/es/

han mantenido varias reuniones con cada referente de protección de datos. A su vez cada referente ha mantenido reuniones con cada responsable de tratamiento para recabar la información necesaria. Corresponde a cada responsable, de acuerdo al principio de responsabilidad proactiva (*Accountability*) que rige el RGPD, decidir el nivel de segregación o agregación con el que desea registrar los tratamientos de datos de carácter personal que requiere su actividad.

Esta toma de datos y posterior análisis de documentación tiene como finalidad, por un lado, conocer si se recogen o tratan datos de carácter personal, y por otro, determinar si existen y se aplican los protocolos necesarios de cumplimiento de las obligaciones jurídicas en cada órgano comprobando su adecuación a la normativa de protección de datos.

Se ha procedido posteriormente a elaborar la información destinada a ser publicada como Registro de Actividades de Tratamiento. El registro recoge la información conforme lo indicado en el artículo 30 del RGPD, determinándose quién es el **responsable** de tratamiento, cuál es su **finalidad** y se proporciona un breve análisis de las bases de **legitimación** del tratamiento analizado.

El tratamiento de datos personales, para ser lícito, debe basarse necesariamente en una de las bases de legitimación previstas en el artículo 6 del RGPD y, en caso de existir tratamientos de categorías especiales de datos, dicho tratamiento deberá basarse en alguna de las bases de legitimación previstas en el artículo 9.2 del RGPD. En caso de que en algún tratamiento se traten datos de categorías especiales de datos, se procederá a analizar la pertinencia y necesidad de tratar tales datos, para lo que se realizará un examen de la proporcionalidad en el tratamiento de dichos datos.

En una segunda fase, se procede a su publicación en la página web. Hay que tener en cuenta que el Registro de Actividades de Tratamiento es un registro dinámico, que será **actualizado frecuentemente** en función de las variaciones que tenga y por tanto, irá teniendo diferentes versiones. La inclusión, supresión o modificación de los tratamientos en el inventario de actividades de tratamiento habrán de ser comunicadas a la Delegada de protección de datos. En un futuro próximo se creará una aplicación que además de incluir el mantenimiento del inventario de actividades de tratamiento, incluirá información relativa a la gestión de riesgos de los tratamientos, evaluaciones de impacto y auditorías.

«La finalidad del registro RAT se basa en el principio de *"responsabilidad proactiva"*, uno de los principios fundamentales del RGPD»

Con respecto a las redes creadas para el óptimo cumplimiento de las obligaciones generadas por el RGPD en la Administración Pública de Euskadi, que es el ámbito que gestiona la Delegada de protección de datos de la CAE, contamos con un total de 112 responsables de tratamiento, 30 responsables de las medidas de privacidad, 37 referentes de protección de datos y actualmente están registrados 802 tratamientos. ❑

Tabla 2: el Registro de Actividades de Tratamiento en cifras

	Responsables de tratamiento	Responsables de medidas de privacidad	Referentes	Registro de Actividades de Tratamiento
Departamentos	94	8	17	573
Org. Autónomos	10	10	12	95
E.P.D.P.	8	12	8	134
Total...	**112**	**30**	**37**	**802**

Delegada de Protección de Datos

Podéis consultar la estructura, funciones y marco legal de la Delegada de protección de datos accediendo a la siguiente página web:

https://www.euskadi.eus/web01-a2datuba/es/contenidos/informacion/estructura_dpd/es_def/index.shtml

ALBOAN:

Consejos sobre Windows10 y Office365: compartir, coedición y control de versiones

«La propia plataforma del Office365 almacena de forma automática todas las versiones que se van generando de un mismo documento»

Como continuación del artículo anterior (publicado en junio), en el que hacíamos una breve introducción del nuevo entorno informático que se está desplegando en todos los puestos del Gobierno Vasco, os traemos esta nueva píldora formativa.

En esta ocasión, os presentaremos una serie de buenas prácticas o consejos útiles para que los tengáis en cuenta a la hora de compartir un documento con otra persona o un grupo de personas colaboradoras (tanto internas como externas).

COMPARTIR

Como ya habíamos comentado, a partir de ahora, en vez de enviar ficheros adjuntos, se recomienda **compartir** los documentos, por varias razones:

- ✓ Se ahorra tiempo
- ✓ Se fomenta el trabajo colaborativo
- ✓ Se tiene un mayor control sobre el documento que vamos redactando
- ✓ Se evitan los problemas que habitualmente se producen al gestionar varias versiones de un mismo documento

El nuevo entorno informático, compuesto por el paquete ofimático Office365 y por el sistema operativo Windows10, nos permite ahorrar tiempo a la hora de compartir un fichero, ya que una vez redactado, podemos compartirlo de varias formas: por ejemplo, haciendo botón derecho del ratón sobre el documento y seleccionando la opción «Compartir». Con idea de garantizar el control del documento, se recomienda establecer una **fecha de caducidad**, a partir de la cual el documento dejará de estar compartido (accesible) para la(s) persona(s) con la(s) que se compartió.

En algunos casos es también muy importante **garantizar la confidencialidad** del documento. Pues bien, el nuevo Office365 nos ofrece una serie de opciones que nos permite asegurar el control del contenido del mismo: por ejemplo, compartirlo con una persona concreta y no permitir el acceso a nadie más. Estas y otras opciones son nuevas funcionalidades que nos ofrece el Office365. Desde aquí os animamos a que las probéis la próxima vez que compartáis un fichero.

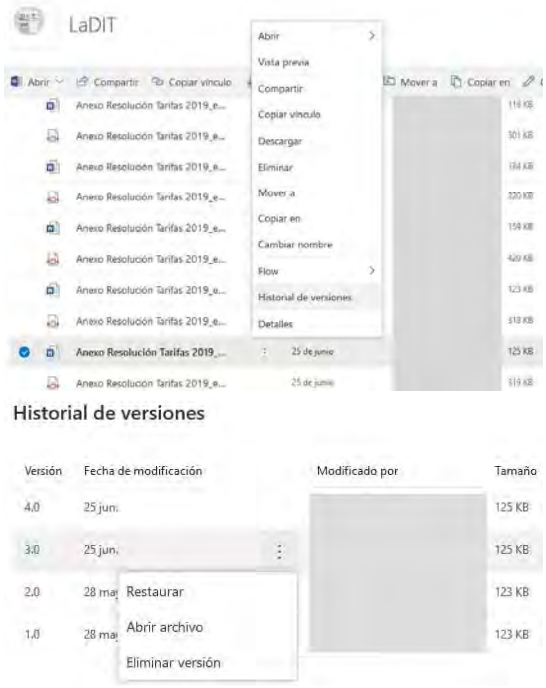
Otra opción que puede ser muy útil para muchas personas que, por las características de su trabajo suponga trabajar en grupo y deban colaborar para redactar un mismo documento, es la llamada **coedición**. Esta funcionalidad permite que dos o más personas puedan editar simultáneamente un mismo documento (un escrito, una hoja de cálculo, etc.). Para ello, se aconseja que ambas personas abran y editen el documento online,

es decir, a través del navegador (Internet Explorer, Mozilla Firefox, Chrome, etc.), lo cual facilitará la sincronización de las modificaciones que lleve a cabo cada persona. Gracias a esta nueva funcionalidad, se puede ver en vivo el párrafo en el que está el cursor de la otra persona e incluso el texto que está escribiendo en ese mismo momento. Con la ventaja, además, de que todas las modificaciones que se hagan quedan registradas sobre ese mismo documento para

cualquier persona que lo consulte posteriormente. Por lo tanto, ya que no es necesario comprobar los cambios realizados por la otra persona e incluir esos cambios en la última versión del documento, tal y como suele ocurrir actualmente en muchas ocasiones, etc. Por lo que al final podemos ahorrar mucho tiempo.

Relacionado con esta última opción, indicar que la propia plataforma del Office365 guarda de forma automática en el propio **Sharepoint** donde está ubicado el documento todas las **versiones** que se van generando. Gracias a ello, si en un momento dado no estamos de acuerdo con los cambios realizados en un documento, podemos revisar el historial de ese archivo y «recuperar» una versión anterior. Para ello, simplemente debemos seguir estos pasos:

1. Seleccionar el documento
2. Pinchar en los tres puntos que aparecen a la derecha del nombre del fichero (o colocar el cursor del ratón encima del nombre del documento correspondiente y pulsar el botón derecho del ratón)



3. En el menú que se despliega, seleccionar *«Historial de versiones»*. (En función de las modificaciones que haya tenido ese documento, el listado de versiones será más o menos extenso)
4. Ahora pinchamos en el desplegable que aparece junto al nombre y tenemos las siguientes opciones: *«Restaurar»*, *«Abrir archivo»* o *«Eliminar versión»*. Si seleccionamos la primera opción, ese documento pasará a ser el documento en curso

Otra opción interesante, y que puede sernos de mucha utilidad, es la que nos permite ver la lista de todos los documentos que, en algún momento, alguien ha **compartido con nosotros/as**, y de los que nosotros/as hemos compartido con otras personas, y que la podemos consultar en nuestro **OneDrive**.

Para acceder a esta opción, habrá que seguir los siguientes pasos:

1. Primero hay que entrar en el portal de Office365 (https://portal.office.com)
2. Ir al OneDrive (se puede acceder pulsando el icono correspondiente que aparece en la pantalla principal)
3. Ahora, en el menú lateral izquierdo de la web, pinchamos en la opción *«Compartido»*
4. Una vez dentro, en la parte superior central de la página aparecen dos pestañas: *«Compartido contigo»* y *«Compartido por el usuario»*
5. Si elegimos la opción *«Compartido contigo»*, por cada fichero se nos mostrarán los siguientes datos: el nombre del fichero que han compartido conmigo, la fecha en la que fue compartido, el nombre de la persona que lo compartió, y la fecha de la última actividad realizada con ese fichero (incluyendo el nombre de la persona que la ha realizado)
6. Si elegimos la opción *«Compartido por el usuario»*, por cada fichero se nos mostrarán los siguientes datos: el nombre del fichero compartido, la ubicación del archivo, y fecha de la última actividad realizada con ese fichero (incluyendo el nombre de la persona que la ha realizado)

Como vemos, el nuevo entorno ofimático Office365 nos ofrece un sinfín de opciones, así que os seguiremos informando en los siguientes números de nuestro boletín Aurrera.

No os los perdáis. ❑

«Una opción muy útil para muchas personas que deben colaborar en la redacción de un mismo documento es la llamada "coedición"»

Web de acceso al portal del nuevo Office365: https://portal.office.com

ALBOAN

¡¡Contraportada!!

Nº 69

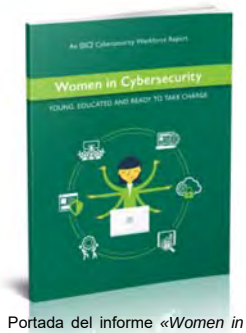
septiembre 2019

AL CIERRE

Las mujeres y la ciberseguridad

A día de hoy, la presencia de las mujeres en el sector de las Tecnologías de la Información sigue siendo todavía menor a la de los hombres, y en el ámbito de la ciberseguridad, en particular, aún menos.

Si bien la presencia de las mujeres en estos puestos de trabajo ha pasado de un 11% a un 25% en menos de dos años , según un reciente estudio de la asociación (ISC)[2] titulado *«Women in Cybersecurity. Young, educated and ready to take charge»*, una de las principales conclusiones es que todavía queda mucho por hacer para alcanzar la equiparación real de puestos y salarios. [Es importante señalar que este estudio sólo ha analizado una muestra de 1.500 puestos de América del Norte, Sudamérica y Asia/Pacífico, y no se ha incluido Europa].



Portada del informe *«Women in Cybersecurity. Young, educated and ready to take charge»* elaborado por la asociación (ISC)[2]

En cuanto a la representación que tienen las mujeres expertas en ciberseguridad en la alta dirección, es importante destacar que ellas ya ganan a los hombres, puesto que representan un 7% como directoras de TI frente a un 2% de los hombres.

En cuanto a los salarios, lo habitual es que entre las personas ejecutivas con más edad y mejor pagadas, las diferencias entre ellas y ellos sea todavía grande a favor de los hombres.

Se calcula que este mismo año, la demanda de empleo se incremente hasta los seis millones de puestos de trabajo en todo el mundo, y que el sector de la ciberseguridad crezca hasta los 152.000 millones de euros en 2020, según otro informe publicado por Society for Human Resources Management. Por todo ello, se considera que la participación de la mujer es clave para poder cubrir la demanda de puestos de trabajo que generará el sector de la ciberseguridad.

Más información en: https://www.isc2.org

PROTAGONISTAS

Ikerbasque premia la labor de las mujeres científicas

La fundación Ikerbasque premia la labor investigadora de las científicas vascas María Isabel Arriortua, Aitziber López Cortajarena y Maia García Vergniory.

La primera edición de este premio se ha dividido en tres categorías:

- ✓ María Isabel Arriortua (1950) ha sido reconocida por toda su **carrera investigadora**. Catedrática de Cristalografía y Mineralogía en la UPV/EHU desde 1992, siendo la primera profesora titular de la UPV/EHU formada en la propia universidad.
- ✓ Aitziber López Cortajarena (1974) ha sido reconocida por su **liderazgo** dentro del ámbito de la ingeniería de proteínas. Tras doctorarse en Bioquímica por la UPV/EHU se trasladó a la Universidad de Yale, en donde trabajó en el diseño, estructura y función de proteínas. En 2016, se unió al CIC biomaGUNE para dirigir el grupo de Nanotecnología Biomolecular.
- ✓ Maia Garcia Vergniory (1978) ha sido reconocida por su **contribución** en el campo de los materiales topológicos. Se doctoró en física de la materia condensada en la UPV/EHU. Posteriormente trabajó en el Max Planck Institute of Microstructure Physics. Actualmente, desarrolla su investigación sobre materiales topológicos en el DIPC.

Con esta iniciativa Ikerbasque intenta visibilizar las carreras de mujeres investigadoras brillantes, reconocer su aportación a la ciencia y, de esta forma, que puedan servir de modelo a las futuras generaciones.

Más información en:
https://www.ikerbasque.net/es/noticias/ikerbasque-reconoce-y-visibiliza-la-labor-de-las-mujeres-investigadoras