EUSKO JAURLARITZA GOBIERNO VASCO

AURRERA!

Nº 63

marzo 2018

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

ÍNDICE

En el mundo de las Nuevas Tecnologías los cambios son constantes y hay que estar preparados. Entre 2018 y 2019 el puesto informático de la Red Corporativa del Gobierno Vasco vivirá una importante migración, en este caso, pasaremos a usar **Windows10 y Office365**. Tal y como se ha podido comprobar en el Proyecto Piloto realizado recientemente, el cambio en algunos aspectos, sobre todo, a la hora de trabajar en Grupo e intercambiar documentos, va a ser importante. Por lo que, tal y como ya hicimos en pasadas actualizaciones, conviene familiarizarnos con las nuevas herramientas/funcionalidades lo antes posible.

Como segundo tema, hablaremos del concepto **IoT**, es decir, de «*Internet de las cosas*», y de todo lo que implica: dónde se puede aplicar, qué nos puede traer en un futuro próximo, etc., pero centrándonos especialmente en los riesgos que puede acarrear sobre la privacidad de las personas. Os avanzamos, además, varias iniciativas en este ámbito que se van a llevar a cabo en el Gobierno Vasco.

Cada vez son más los peligros que nos acechan en Internet. Y dado que el daño que podemos sufrir (tanto las personas particulares como las empresas vascas) es cada vez más importante, el Gobierno Vasco, a través de la SPRI ha decidido crear una entidad que pueda realizar un trabajo de prevención y protegernos de los ataques de los ciberdelincuentes. En el apartado de «Alboan», por tanto, os presentamos el «Centro Vasco de Ciberseguridad», también conocido por sus siglas en inglés, **BCSC** (*Basque Cybersecurity Centre*).

En el apartado «*Contraportada*», y para acabar este nuevo ejemplar del boletín, os comentamos, por una parte, la importancia que tendrá la **accesibilidad de los sitios** web y aplicaciones para dispositivos móviles de los organismos del Sector Público, todo ello a raíz de la Directiva 2016/2012 del Parlamento Europeo y del Consejo, de 26 de octubre de 2016. Y, por otra parte, incluimos una reseña sobre una de las más importantes figuras en el ámbito de la informática: **Ada Lovelace**. No os perdáis su historia (que podéis ampliar consultando el enlace que se incluye).

Windows10 y Office365

A lo largo de los próximos meses se irán actualizando el sistema operativo y el paquete ofimático de todos los ordenadores del Gobierno Vasco. Ello supondrá un cambio importante desde el punto de vista de la forma de trabajar en nuestro día a día.

[1] **Boletín Aurrera:** para más información, podéis consultar en el boletín Aurrera nº 62 (de diciembre de 2017) el artículo titulado «*Llega el Office365*»]

[2] **Gestión del Cambio:** para conocer cómo se organiza y en qué consiste un Plan de Gestión del Cambio, podéis consultar en el boletín Aurrera nº 30 (de junio de 2008) el artículo titulado «*Saber gestionar (bien) el cambio*»]

2018 y 2019 va a ser un periodo lleno de cambios para el Puesto Informático base del Gobierno Vasco, tal y como ya os adelantamos en el anterior boletín Aurrera[1].

Como consecuencia de ello, nuestros ordenadores pasarán del actual sistema operativo Windows7 al Windows10, así como al nuevo paquete ofimático de Microsoft, el llamado «*Office365*».

CONTEXTO

Actualmente, y según todos los estudios, nos encontramos en la llamada «*Cuarta Revolución Industrial*», la cual se basa en la tecnología aplicada a los procesos de producción de las organizaciones.

Esta nueva revolución está provocando un importante cambio organizativo, donde los dispositivos móviles y las herramientas para colaborar en equipo están cada vez más presentes y tienen cada día más importancia.

Esta época que nos ha tocado vivir se caracteriza por:

- La adopción masiva de dispositivos móviles por parte de las personas
- La información siempre debe estar disponible
- La gran presencia que tienen las Redes Sociales en los negocios
- La facilidad de uso de los nuevos dispositivos

El nuevo entorno que se va a implantar (Windows10+Office365) se basa, por un lado, en ofrecer sus servicios en la «*nube*», lo cual nos va a permitir tener acceso a todos nuestros documentos desde cualquier lugar y en cualquier momento; y, por otro lado, en que las licencias ya no son por puesto de trabajo, sino que pasan a ser por persona y multidispositivo.

«En EJIE se ha llevado a cabo un Proyecto Piloto con 210 personas.»

[ver cuadro «*Licencias y productos Microsoft*»]

GESTIÓN DEL CAMBIO

Dado el alcance del proyecto de migración que se va a llevar a cabo (que afectará a todo el personal de la Red Corporativa Administrativa del Gobierno Vasco [Departamentos y Organismos Autónomos]), alrededor de **7.000 personas** en total, es necesario llevar a cabo una buena Gestión del Cambio[2], para conseguir entre otros los siguientes objetivos:

- ✓ Potenciar el liderazgo activo de la Alta

Dirección, lo cual facilitará la marcha del proyecto

- ✓ Alinear a los profesionales de la organización con los objetivos del proyecto, evitando de esta forma malentendidos
- ✓ Buscar el compromiso de todo el personal, lo cual favorecerá el éxito del proyecto
- ✓ Ayudar a superar las «*resistencias al cambio*» que suelen surgir
- ✓ Acercar la tecnología al funcionamiento del día a día y, de esta forma, aprovechar mejor los recursos
- ✓ Acompañar a las personas en el proceso de cambio

En definitiva, el objetivo del proyecto (bautizado como «*Proyecto ERA*») es facilitar a todo el personal de la organización, en este caso, Gobierno Vasco y EJIE, la adopción de las nuevas herramientas o funcionalidades.

PROYECTO PILOTO EN EJIE Y GOBIERNO VASCO

En mayo de 2017 **EJIE** publicó un Pliego de Bases Técnicas para llevar a cabo un Proyecto Piloto[3] (que incluía la Gestión del Cambio asociado) para aplicarlo a su personal. Dicho Piloto permitirá comprobar el funcionamiento de las nuevas aplicaciones en nuestra Red Corporativa, así como detectar los problemas que pueden surgir cuando se migren todos los puestos ofimáticos del **Gobierno Vasco.**

[3] **Proyecto Piloto de EJIE:** para más información sobre el contenido del Pliego de Bases Técnicas publicado por EJIE, podéis consultar en su página web el expediente titulado «*Servicios para la Gestión del Cambio sobre Office 365 en EJIE*» (Expte. nº EJIE-039-2017)

Web de EJIE:

http://www.ejie.eus

(apartado «*Perfil de Contratante*»)

Licencias y productos Microsoft

Todo el personal de la Red Corporativa del Gobierno Vasco dispondrá en su puesto de trabajo del Windows10 como sistema operativo. Mientras que en el caso del paquete ofimático, junto al LibreOffice, se instalará el Office365. Dado que existen distintas versiones y licencias se han definido varios perfiles:

Generalista:

- **Office365ProPlus**. El correo electrónico, *Sharepoint*, etc. se queda *OnPremise* (se instala en modo local en cada PC), pero se tiene OneDrive (disco en la nube con 1 TB de capacidad de almacenamiento) y da la posibilidad del Office Professional en el puesto (hasta 5 PCs, 5 *tablets* y 5 móviles).

  Se entiende que estos usuarios/as no tienen grandes necesidades de colaboración, seguridad o movilidad.

Especialista:

- **Office365 E3**. se trata de una versión con los programas «*offline*». Además de lo que incluye el Generalista, el correo electrónico, *Sharepoint*, *OneDrive*, etc. estarían en la nube.

  Ofrece mayores posibilidades de colaboración, seguridad, capacidades de almacenamiento, movilidad y Office Professional en el puesto (también con 5 instalaciones en cada dispositivo).

Especialista Móviles:

- **Office365 E1**: igual que el E3 pero sin disponer el Office Professional. Se trata de un entorno exclusivamente online, por lo que el correo electrónico, *Sharepoint*, etc. estaría en la nube.

  A partir del segundo año y son unos 350, se entiende que NO necesitan Access en el puesto.

El proyecto piloto ha tenido una duración de 5 meses, y se ha desarrollado entre finales de 2017 y principios de 2018.

Los objetivos inicialmente planteados han sido los siguientes:

- ✓ Superar las resistencias habituales al cambio que presentan las personas, «*acompañándolas*» y dándoles el soporte necesario antes y después de la migración
- ✓ Mostrar las mejoras que ofrecen las nuevas herramientas tanto para las personas usuarias como para la organización

[4] **EJIE:** para conocer la organización, servicios que actualmente ofrece y el funcionamiento de la Sociedad Informática del Gobierno Vasco, EJIE S.A., podéis consultar su página web:

http://www.ejie.eus

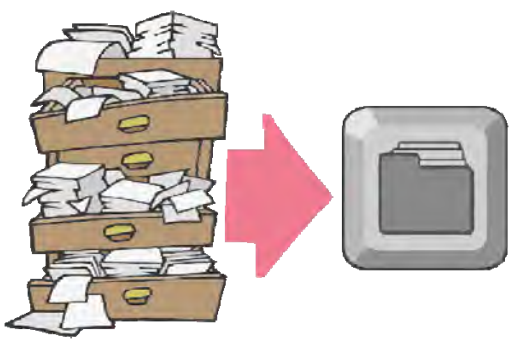
«El nuevo entorno (Windows10+Office365) ofrece sus servicios en la "nube", lo cual nos va a permitir tener acceso a todos nuestros documentos desde cualquier lugar y en cualquier momento.»

- ✓ Mejorar la realización de las funciones ofimáticas, especialmente a la hora de compartir y gestionar los ficheros
- ✓ Acompañar y facilitar la asunción de las nuevas tecnologías por parte del personal
- ✓ Integración del nuevo Office365 con los procesos operativos de EJIE/Gobierno Vasco.

El ámbito de aplicación del Piloto ha abarcado a todo el personal de EJIE (**210 personas**, en total), así como a un pequeño grupo del Gobierno Vasco.

En el caso de EJIE[4], las 210 personas implicadas se han dividido en 3 grupos:

- Dirección, Administración y Auxiliares Administrativos
- Áreas de Sistemas y Producción
- Área de Proyectos y Asistencia Técnica

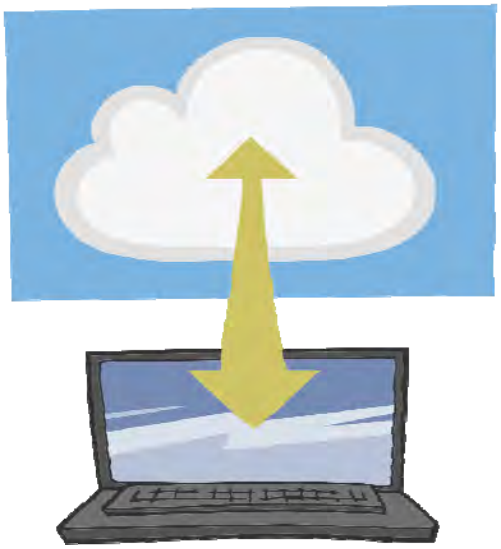


Además de estos grupos, existe otro colectivo importante, el personal del equipo de Técnicos de Sistemas y el Centro de Atención a las personas Usuarias (CAU), ya que son ellos los que se encargarán del soporte una vez concluya la fase de Gestión del Cambio. De ahí su importancia.

MIGRACIÓN DE FICHEROS

Con idea de probar todos los productos que ofrece el nuevo paquete ofimático Office (tanto en su versión *online* como *offline*), se han instalado los paquetes o *suites* Office365ProPlus, Office365 E1 y el Office365 E3.

Para poder validar las nuevas funcionalidades de la forma más real posible, las personas que han participado en el Proyecto Piloto han tenido que migrar sus buzones de correo electrónico a la nueva plataforma web y sus documentos a los nuevos entornos (Sharepoint y OneDrive).



Como es sabido, actualmente todo usuario/a de la Red Corporativa del Gobierno Vasco dispone de una unidad de red (denominada **Disco M**, «*Mío*»), destinada a albergar en ella información o documentos considerados personales, y otra unidad (**Disco N**, «*Nuestro*») utilizado principalmente como espacio para

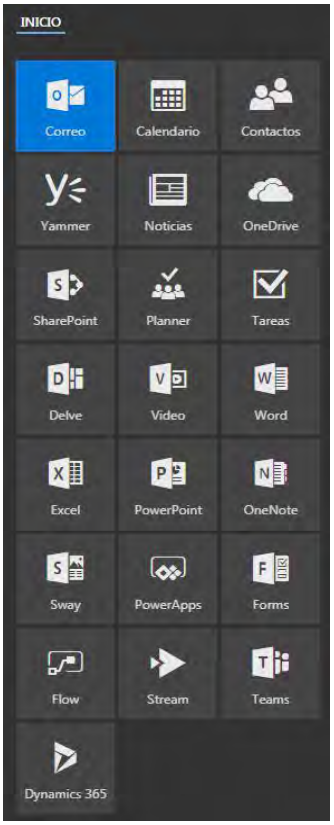
el trabajo en grupo e intercambio de archivos. Pues bien, uno de los primeros pasos que se ha llevado a cabo ha consistido en migrar los ficheros personales (los ubicados en la unidad M) al nuevo espacio personal que todas las personas tienen/tendrán en OneDrive.

Por lo tanto, se dejarán de usar los servidores de ficheros o unidades de red habituales y se pasará a usar soluciones en la «nube».

VALORACIONES

Una vez concluido el Proyecto Piloto de EJIE, algunas de las conclusiones que han expuesto las personas que han participado han sido las siguientes:

- Desde el punto de vista funcional, el nuevo Office365 va a suponer un cambio importante
- Dadas las nuevas funcionalidades que ofrece el Office, los usuarios/as tienen miedo a perder información
- A la hora de realizar el trabajo diario, hay que cambiar la forma de trabajar e intercambiar ficheros y documentos con otras personas



Con objeto de abordar las incidencias detectadas, se ha decidido elaborar un «*Plan de Actuación*» para definir los siguientes elementos:

- ✓ **Normativas y políticas** de funcionamiento para cada uno de los colectivos afectados
- ✓ Plan de **comunicación** previa y durante la transición al nuevo entorno
- ✓ Plan de **formación**
- ✓ **Soporte y ayuda** posterior a la migración

Con todo ello, se quiere facilitar el cambio al nuevo entorno informático, así como resolver aquellas dudas o problemas que puedan surgir durante la migración. Todo ello para conseguir que la implantación del nuevo software sea un éxito y podamos sacarle el mayor provecho.

En este tipo de proyectos tan importante es la solución informática/tecnológica elegida como llevar a cabo una buena gestión del cambio para que el proyecto tenga éxito.

UNA NUEVA ERA

En definitiva, la implantación de la plataforma Office365[5], de Microsoft nos permitirá tener acceso a la información en tiempo real, desde cualquier lugar, en cualquier momento y desde cualquier dispositivo, optimizará nuestras operativas de trabajo al poder coeditar los documentos de manera simultánea entre varias personas y potenciará la colaboración y el trabajo en equipo entre aquellos que compartimos información con varias personas, de una forma segura.

Con esta iniciativa, el Gobierno Vasco y EJIE se suman al proceso de cambio que actualmente está presente en la mayoría de las organizaciones que avanzan hacia la **nueva Era Digital** («*ERA, berri baten lanean*») en la que nos encontramos. ❑

O365 Era
Berri baten lanean

[5] **Office365**: algunas de las aplicaciones que incluye la suite Office365 son las siguientes:
Paquete ofimático: que incluye **Word**, **Excel**, **PowerPoint**, **Outlook** *on-premise* (5 GB de capacidad), **Access** y **OneNote**.
OneDrive (1 TB para almacenar documentos).
Outlook web (servicio de correo online, ofrece una capacidad de 100 GB de almacenamiento).
Skype (servicio para conectar con otras personas a través de video llamadas, llamadas de voz, mensajería, etc.)
SharePoint (herramienta de trabajo colaborativo)
Yammer (red social privada para empresas)
Teams (herramienta para grupos de colaboración)
Delve (buscador de documentos/ficheros y organizador de información)
Planner (para organizar y planificar las tareas de un equipo de trabajo).

Internet de las cosas (IoT)

Internet de las cosas (en inglés *The Internet of Things*, abreviado *IoT*) se ha convertido en un término familiar que aparece con asiduidad en los medios de comunicación, también es un término que está en constante evolución. Así que vamos a ver en qué consiste.

Se espera que para el año 2020 existan cerca de 20 billones de «cosas» conectadas a Internet.

Estas «cosas» no serán dispositivos de propósito general, tales como ordenadores y teléfonos inteligentes, sino objetos de propósito o funciones específicas, como, por ejemplo, las máquinas expendedoras de bebidas y alimentos, frigoríficos, dispositivos para el control de la salud de las personas, de tele-ayuda, encimeras de cocina, marcapasos...

Se entiende por «cosa» cualquier objeto, natural o artificial, al que se le puede asignar una dirección IP[6], y que tiene la capacidad de transmitir información a través de Internet.

La Internet de las cosas tiene gran impacto en la economía y está creando nuevos modelos de negocio y transformando otros muchos, algunos de ellos de una manera abrupta, ya que en algunos casos no se sabe cómo lidiar con estos cambios.

¿QUÉ ES IOT?

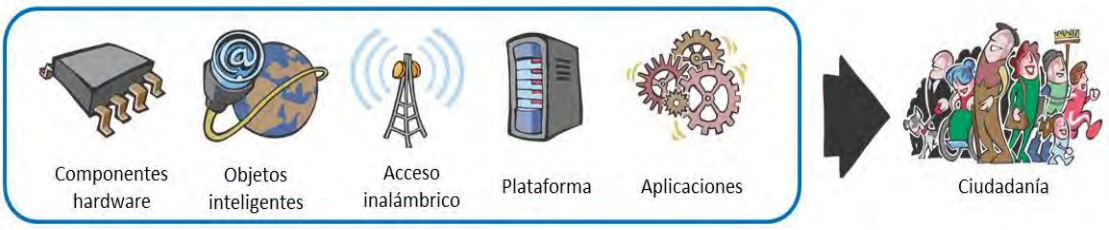
Es una red de objetos físicos (cosas) dedicados que contienen tecnología incorporada, normalmente embebida (incrustada), para comunicarse o interactuar con sus estados internos o con su entorno exterior, y que están conectados a Internet. Gracias a ello se capturan datos y eventos (se recolectan información de todo tipo), y gracias a estos datos y eventos se puede aprender, actuar de una forma proactiva, o de una manera preventiva, transformar procesos, estudiar comportamientos... y todo lo que seamos capaces de imaginar. Por ejemplo, sensores que controlan el desgaste de las pastillas de los frenos de un aparato de locomoción, si bien dichas pastillas tienen una vida útil, existen factores externos que pueden alargar o acortar dicha vida útil, como pueden ser las temperaturas que soportan, la capacidad de disipación de la energía, el número de veces que se accionan por kilómetro... para una flota de trenes estos datos pueden suponer aumentar la seguridad del transporte de pasajeros.

«El objetivo de un sistema basado en IoT es la recolección y gestión de datos, para su posterior explotación»

Resumiendo, podemos decir que gracias a Internet de las cosas los objetos transformarán nuestra vida cotidiana facilitándonos las tareas que tenemos que realizar.

INICIOS DE LA IOT

En un principio, el término «*Internet of Things*» fue acuñado por las personas



[6] **Dirección IP:** es un número que identifica la interfaz que se conecta a Internet: cada dispositivo que se conecta a Internet realiza dicha conexión/comunicación a través de una interfaz utilizando el protocolo IP (*Internet Protocol*, Protocolo de Internet).

Estas direcciones pueden ser dinámicas (varían). Existen direcciones IP **públicas** (asignadas por el Proveedor de Servicios de acceso a Internet o IPS), y direcciones IP **privadas**, asignadas dentro de una red privada, como la red que una persona puede configurar en su propia casa.

Las direcciones IP están compuestas por cuatro números enteros (4 bytes) entre 0 y 255 (en hexadecimal, 0 y FF, respectivamente), escritos en el formato xxx.xxx.xxx.xxx.

Hay tres rangos que se reservan exclusivamente para las IP privadas, y que son los siguientes:

- ✓ **Clase A**: 10.0.0.0 a 10.255.255.255.
- ✓ **Clase B**: 172.16.0.0 a 172.31.255.255.
- ✓ **Clase C**: 192.168.0.0 a 192.168.255.255.

desarrolladoras de tecnología basada en RFID[7], sobre finales del siglo XX, y se basaba en la obtención de información respecto a un objeto etiquetado realizando una consulta en Internet (los objetos, en este entorno RFID, tienen un identificador único, la etiqueta RFID, y los lectores hacen un seguimiento de estos objetos etiquetados, con lo cual tenemos un mapa conceptual o virtual de lo que realmente está ocurriendo). Más tarde estos conceptos se fusionaron con lo que se conoce como «*computación ubicua*».

EL SALTO AL ENTORNO FÍSICO

La computación ubicua es la integración de la informática en el entorno de la persona, es decir, que ésta no dependa de una pantalla, que los ordenadores no se vean como elementos diferenciados, sino que estén integrados en el entorno.

El informático americano **Mark Weiser**[8] introdujo el concepto de computación ubicua, y acuñó el término intentando englobar los diferentes dispositivos diseñados en función de cuatro principios:

1. El propósito de un dispositivo informático es ayudarte a hacer alguna cosa (las personas son ayudadas por la tecnología)
2. El mejor dispositivo es aquél que pasa desapercibido (las personas no son conscientes de que están siendo ayudadas)
3. Los dispositivos deben extender tu inconsciente (las personas interaccionan con los objetos de la forma más natural)
4. La tecnología tiene que aportar calma y bienestar. (las personas aceptan estas tecnologías)

Mark Weiser resumió estos principios en la siguiente frase:

«***Las tecnologías más profundas son aquellas que desaparecen, se tejen a sí mismas en la tela de la vida diaria hasta que son imposibles de distinguirse de ésta***», es decir, que se convierten en una parte esencial e indistinguible de los objetos cotidianos; Internet da el salto de los dispositivos tradicionales a los objetos cotidianos, al entorno real.

RIESGOS

Existen riesgos asociados a *Internet of Things*; su principal característica es que se conecta a Internet, y ésta también es su principal debilidad, que una persona atacante modifique de forma remota la configuración de un dispositivo (sensor) o su propia funcionalidad puede tener consecuencias graves, según cuál sea el propósito de dicho sensor (un sensor puede estar incluido desde en un juguete con conexión a Internet hasta en una central de producción de energía nuclear).

Con la IoT la superficie de ataque (suma total de las vulnerabilidades posibles) se multiplica de una forma exponencial. Internet de las cosas presenta un campo perfecto para realizar delitos cibernéticos, por eso es necesario establecer medidas de protección para mitigar los riesgos a los que están expuestos los sistemas que utilizan Internet de las cosas.

Las personas atacantes buscan objetivos a través de Internet (dispositivos a los que puedan acceder y administrar de forma remota) y de esta forma realizar las actividades ilícitas que deseen (por ejemplo, inutilizando servidores Web mediante la utilización masiva de dispositivos IoT, a través de ataques DDoS[9]).

Cuando se instala un dispositivo IoT la primera recomendación es cambiar la contra-

[7] **RFID:** para más información podéis consultar el boletín Aurrera nº 42 (junio 2011).

[8] **Mark Weiser:** Ideólogo de la computación ubicua, fue un informático que estudió «*Ciencia de la Comunicación y la Informática*» en la Universidad de Michigan.

Según Weiser la historia de la computación podría dividirse en tres eras:

- La de los ordenadores centrales *(mainframes)*
- La de los ordenadores personales
- La de la computación ubicua

Lo curioso es que esto lo manifestó a finales de los años 80.

[9] **DDoS:** *Distributed Denial of Service*, es lo que se conoce como Denegación de Servicios Distribuida, y consiste en generar una cantidad masiva de peticiones al servidor desde diferentes orígenes a la vez, con el objetivo de inhabilitarlo temporalmente.

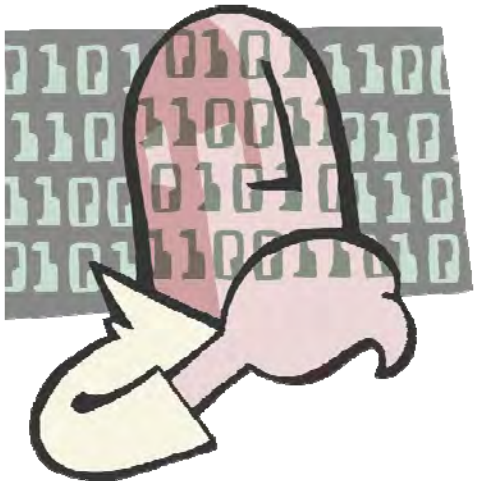
seña que viene instalada por defecto seleccionando una realmente segura para todos sus perfiles (especialmente para el perfil de Administrador), si esto no es posible, se debería cuestionar la instalación de dicho dispositivo.

PRIVACIDAD

Uno de los problemas que existen cuando hablamos de Internet de las cosas es el de la privacidad. Las comunicaciones seguras son fundamentales para preservar la privacidad; podemos realizar comunicaciones seguras, pero los pequeños dispositivos no suelen utilizar los protocolos para que así sea, bien por su poder de procesamiento, que no suele ser muy grande (tienden a ser elementos que consumen muy poca energía), bien porque encarece el producto.

Por otro lado, debemos ser conscientes de que somos medidos por sensores, y poder decidir que no lo seamos, si así lo deseamos, o aparecer como personas anónimas.

Respecto al almacenamiento de los datos recogidos por estos sensores, es fundamental preservar la Integridad[10] y Confidencialidad[11] de la información almacenada, y que esta información no contenga datos sensibles; para preservar estas garantías existen mecanismos que se pueden aplicar. En lo que respecta al procesamiento de los datos almacenados (lo que se conoce como «*minería de datos*»), también existen mecanismos para asegurar la privacidad.



Y, por último, se nos puede localizar, seguir e identificar, por lo que es necesario que se avise a la persona usuaria que esto es así, para que sea consciente de estos procesos que se están realizando sobre su persona, y, si

[10] **Integridad**: asegura que la información no se ha transformado ni modificado de forma no autorizada durante su procesamiento, transporte o almacenamiento, detectando fácilmente posibles modificaciones que pudieran haberse producido.

[11] **Confidencialidad**: previene contra la puesta a disposición, comunicación y divulgación de información a personas, entidades o procesos no autorizados.

SOFIA2

SOFIA2 (*Smart Objects For Intelligent Applicattions*) es un proyecto tecnológico dentro de la iniciativa europea «I+D Artemis» de tres años (finalizado en marzo de 2012) en el que participaron 19 *partners* de cuatro países de la Unión Europea, incluyendo Indra, Nokia, Philips, Fiat y Acciona. **Es un *middleware* que permite la interoperabilidad de múltiples sistemas y dispositivos**, ofreciendo una plataforma semántica que permite poner información del mundo real a disposición de aplicaciones inteligentes (*Internet of Things*), es multilenguaje y multiprotocolo, permitiendo así la interconexión de dispositivos heterogéneos (los sensores «hablan» diferentes lenguajes con distintos protocolos), también proporciona mecanismos de publicación y suscripción, facilitando la orquestación de sensores y actuadores para monitorizar y actuar sobre el entorno.

SOFIA2 es *open-source*, multiplataforma (Windows, Android, Linux, iOS...), multilenguaje (Java, C, C++, C#, J2ME...), multiprotocolo; también proporciona herramientas visuales de desarrollo para la creación de aplicaciones de forma sencilla.

La arquitectura funcional se basa en áreas colaborativas de dispositivos que intercambian información entre ellas (*Smart Space*), cuyo núcleo central es el SIB (*Semantic Information Broker*), que actúa como elemento de integración de la información intercambiada por los dispositivos.

+info: http://sofia2.com

lo desea, desista, que interrumpa esas acciones y procesos.

La recolección masiva de nuestros datos y metadatos es una forma de vigilancia digital que puede ir en contra de nuestra intimidad y libertad personal.

«La calidad de un dispositivo IoT se mide por las medidas de seguridad que ha implementado el fabricante»

DESARROLLO DE UN SISTEMA BASADO EN LA IOT

Generalmente, los componentes de un sistema basado en Internet de las cosas son los siguientes:

- **Sensores**: se deben elegir los sensores adecuados para la tarea que se quiere realizar. Esta es la capa que se denomina de detección.
- ***Middleware***: es una capa software que conecta componentes software y hardware ocultando todo aquello que resulte no necesario para su comunicación. Es una capa que simplifica el desarrollo de nuevos servicios y su integración con los ya existentes, también es una capa que realiza las funciones de interfaz («entiende» y pone en comunicación los distintos protocolos que se utilizan), para ello utiliza comunicaciones síncronas (en tiempo real) o asíncronas (en diferido), es adaptable y resistente y debe incluir la seguridad respecto a las comunicaciones.
- Una capa de **transporte** (gracias a esta capa los sensores se comunican con el *middleware*), puede ser WiFi, 3G/4G, *mesh radio*[12], satélite, protocolo 6LowPAN[13]… es la capa de intercambio de datos, que se transmiten de una forma transparente a través de las redes de comunicaciones.
- Una capa de **explotación** de los datos capturados (puede estar incluida en el *middleware*). Es la capa de integración de la información: se procesa la información recolectada, se filtra los datos no deseados (se utilizan técnicas que reducen el «ruido» de los datos recolectados) y transforma la información principal en conocimiento útil, tanto para los servicios como para las personas usuarias finales.

GESTIÓN DE DISPOSITIVOS IOT

Gestionar un dispositivo IoT (un sensor) consiste en que se puedan realizar una serie de acciones importantes para la seguridad y para la privacidad, como, por ejemplo:

- Desconectar un dispositivo robado.
- Actualizar el software de un dispositivo y sus credenciales de seguridad.
- Autorizar o denegar remotamente algunas capacidades del hardware .
- Localizar dispositivos perdidos.
- Limpiar información confidencial de un dispositivo robado.
- Reconfigurar parámetros de WiFi, GPRS u otras redes de una manera remota.
- Analizar y auditar el control de acceso.

Se deben extremar las medidas de seguridad respecto a quién se puede conectar al dispositivo (control de accesos), desde qué dispositivo (ordenador personal, móvil, tableta…) y en qué momento (hora del día, de la semana o del año).

LA IOT EN EL GOBIERNO VASCO

Antes de acabar, indicar que en el Gobierno Vasco, fruto de la estrecha colaboración entre las sociedades públicas **EJIE** e **Itelazpi**, ya se están llevando a cabo varios proyectos piloto[14] que utilizan la tecnología de Internet de las cosas, como, por ejemplo, una red de sensores para medir el consumo eléctrico en edificios corporativos; y la utilización de sensores en las zonas de aparcamiento con barrera del complejo de Lakua, con el fin de indicar la disponibilidad de plaza de aparcamiento. De todos ellos os daremos en breve más información. ❑

[12] ***Mesh radio***: red de comunicaciones formada por nodos de radio organizados en malla.

[13] ***6LowPAN***: (acrónimo inglés de IPv6 *Over Low power Wireless Personal Area Networks*). Permite usar IPv6 sobre redes basadas en el estándar IEEE 802.15.4.

[14] ***Proyectos piloto***: se realizarán 2 proyectos:

1. Para gestionar el aforo del parking de Lakua del Gobierno Vasco en Vitoria-Gasteiz (Araba). **Itelazpi** se encargará de diseñar y desplegar la red IoT y **EJIE** de desarrollar los aplicativos.
2. Junto con el Consorcio de Aguas de Bilbao, estará dirigido a la medición de contadores de agua. En este caso, **Itelazpi** se encargará de la red y el Consorcio de los aplicativos.

Para la selección de la mejor tecnología, Itelazpi se ha apoyado en la **Escuela de Ingeniería de Bilbao**, quién ha recomendado el uso de **LoRa** (*Low-range, Low-power*), caracterizada por proporcionar una red de largo alcance y bajo consumo (LPWAN).

ALBOAN:

Centro Vasco de Ciberseguridad (BCSC)

«El BCSC tiene su sede en el Parque Tecnológico de Araba»

En septiembre de 2017 echaba a andar el Centro Vasco de Ciberseguridad (en inglés, Basque Cybersecurity Centre —*BCSC*—), que tiene su sede en el Parque Tecnológico de Araba (Euskadi).

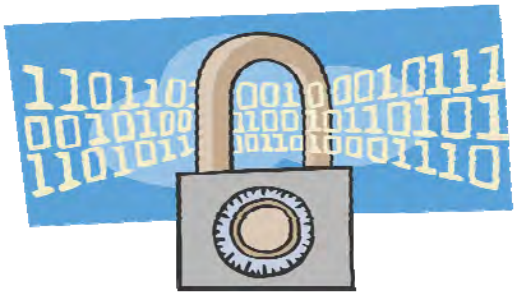
¿Por qué se ha creado el BCSC?

La sociedad ha cambiado, Internet ha transformado la manera de relacionarse, de gobernar y de hacer negocios. El Gobierno Vasco ha puesto en marcha el Centro porque desea que sus empresas sigan siendo competitivas e innovadoras, porque desea que sus ciudadanos/as tengan más recursos para proteger su privacidad, porque desea ofrecer servicios públicos confiables y, en resumen, porque desea que Euskadi siga siendo un ejemplo de sociedad avanzada. El BCSC desea contribuir a que todas las iniciativas orientadas a conseguirlo se lleven a cabo de manera coordinada.

¿Cuáles son sus objetivos?

Su prioridad son las empresas, que serán el foco de su operación habitual. En relación con la ciudadanía la actuación será estructural, es decir, no se dirigirá a resolver situaciones personales sino que trabajará, por ejemplo, en la mejora de los medios con los que la Ertzaintza actúa para perseguir los ciberdelitos, y colaborar con Educación para formar futuros profesionales de la ciberseguridad y ciudadanos/as mejor preparados para el ámbito digital.

En referencia a los servicios que pueden ir dirigidos a la ciudadanía, cuya orientación es más bien ayuda en problemas domésticos, etc., se considera que ya existen servicios públicos consolidados como, pueden ser, la Oficina de Seguridad del Internauta (OSI) o la Internet Segura for Kids (IS4K) ofrecidos por INCIBE, servicios todos ellos que se darán a conocer y se acercarán a la sociedad vasca.



Además, uno de los objetivo del BCSC es ingresar en el **foro global FIRST** de equipos de respuesta a ciberincidentes. La idea es incorporarse a su red, de ámbito mundial, para poder compartir información que permita identificar lo antes posible una amenaza dirigida que pudiera tener impacto sobre sectores estratégicos de la economía vasca, sus infraestructuras críticas o su ciudadanía. También para estar al tanto de las estrategias más eficaces y avanzadas para protegerse. Con ello se persigue el doble objetivo de proteger Euskadi y de contribuir a la comunidad internacional aportando nuestras experiencias en aquellos ámbitos donde seamos referentes o por aprendizaje en incidentes sufridos.

¿Cómo se organiza?

El BCSC tiene ya en su plantilla a 4 personas

especializadas en Ciberseguridad. Además de ello, cuenta con el soporte de la **SPRI** para el asesoramiento en materia jurídica, comunicación corporativa, mecanismos de gestión de la calidad y canales para la formación. Igualmente, en cuanto finalice la obra de acondicionamiento que se está llevando a cabo, dispondrá de 8 personas investigadoras que abordarán proyectos de transferencia de tecnologías de ciberseguridad a la Industria 4.0, 2 agentes de la **Ertzaintza** pertenecientes

ZIBERSEGURTASUN EUSKAL ZENTROA
CENTRO VASCO DE CIBERSEGURIDAD

a la Brigada de Investigación Criminal y un enlace con EJIE. También se ha colaborado con la Viceconsejería de Formación Profesional para definir el programa de formación al profesorado.

Por último, el BCSC es activo en organizaciones europeas orientadas al desarrollo de proyectos de Ciberseguridad y a dar visibilidad a las capacidades de Euskadi en este campo.

¿Qué tipo de servicios va a ofrecer?

Las tareas que se están realizando desde octubre son, por un lado, escuchar y asesorar a quien tenga un incidente de seguridad y, por otro, impartir sesiones de formación y sensibilización a profesionales y empresas. Además, a través de sesiones como puede ser el *Basque Industry 4.0 Meeting Point* se trata de contribuir a crear una conciencia que eleve la cultura de ciberseguridad en nuestro entorno. También se está dotando de la infraestructura necesaria para en el futuro ofrecer otros servicios avanzados que requieren más madurez. En breve publicarán su **portal web**, que será su principal herramienta de comunicación con la sociedad y donde, además de otra información de interés, se describirá la manera de contactar con el BCSC y acceder a sus servicios.

¿Cómo va a funcionar el BCSC?

Los Responsables del proyecto consideran que su valor principal debería orientarse a la detección precoz de ciberamenazas, a la diseminación de buenas prácticas de preparación y a la comunicación de estrategias de respuesta eficaces. Las fronteras más importantes, en cuanto a su capacidad de acción, vendrían dadas por dos circunstancias: en primer lugar, el BCSC no tiene ni tendrá visibilidad de las infraestructuras TIC internas de las organizaciones y, en segundo lugar, no desea competir con la industria ofreciendo actuaciones o servicios que amenacen su actividad. Lo ideal sería que en el futuro las empresas vascas sólo acudiesen a los servicios públicos para pedir ayuda de manera excepcional porque prácticamente todas tengan ya contratados servicios especializados y que los servicios que se prestasen desde el ámbito público fuesen de naturaleza más proactiva como los mencionados anteriormente.

¿Qué relación tendrá con el Gobierno Vasco?

Es importante señalar que el BCSC no nace como un CERT específico para la Administración Pública, si bien encuentra espacios de complementariedad naturales con los organismos correspondientes responsables de la informática de la Administración Pública Vasca, como son la DIT, EJIE, la Dirección de Gestión de Telecomunicaciones y Sistemas Informáticos del Departamento de Seguridad, Izenpe o agentes como las empresas de informática de Diputaciones y Ayuntamientos. Por ello, se está trabajando en un modelo de **colaboración** para contribuir a enriquecer las capacidades de estos organismos sin interferir en sus competencias. ❑

«Uno de los objetivo del BCSC es ingresar en el foro global FIRST de equipos de respuesta a ciberincidentes»

¡¡Contraportada!!

Nº 63

marzo 2018

AL CIERRE

Accesibilidad de los sitios web y aplicaciones para dispositivos móviles del Sector Público

Antes del 23 de septiembre de 2018 se debe transponer la **Directiva (UE) 2016/2012 del Parlamento Europeo y del Consejo, de 26 de octubre de 2016**, sobre la accesibilidad de los sitios Web y aplicaciones para dispositivos móviles de los organismos del Sector Público, que entró en vigor el 22 de diciembre de 2016; por ello, en febrero se abrió un plazo para realizar el trámite de audiencia e información pública y recepción de aportaciones respecto al Real Decreto que regulará este tema.

Este Real Decreto sustituirá y mejorará las condiciones que se exigen a los **portales** de las administraciones públicas en el Real Decreto 1494/2007.

La Directiva Europea dice que «*la **accesibilidad** debe entenderse como un conjunto de principios y técnicas que se deben respetar a la hora de diseñar, construir, mantener y actualizar los sitios Web y las aplicaciones para dispositivos móviles para que sean más accesibles a las personas usuarias, en particular a las personas con discapacidad*», y tiene como objetivo «*garantizar que los sitios Web y las aplicaciones para dispositivos móviles de los organismos del sector público sean más accesibles, al basarse en requisitos comunes de accesibilidad*».

Como dice la Directiva, no se pretende que los sitios Web y las aplicaciones para dispositivos móviles se limiten a publicar única y exclusivamente contenidos accesibles, sino que estos contenidos no accesibles deberán ir acompañados, en la medida de lo posible, de alternativas accesibles; por ejemplo, ante información visual, como planos o mapas, se debe ofrecer una alternativa accesible, como la dirección postal, las paradas de transporte público cercanas, o nombres de lugares y regiones.

http://eur-lex.europa.eu/

PROTAGONISTAS

ADA, pionera de la era digital

Los datos y el software de código abierto, como *Firefox* y *Wikipedia*, son la base de Internet y la tecnología moderna. Compañías como *Google* y *Facebook* dependen del código abierto y webs tan populares como Wikipedia funcionan con datos abiertos. Desde el **14 de octubre de 2014**, se celebra el **Día de Ada Lovelace**, se trata de una celebración internacional de los logros de las mujeres en Ciencia, Tecnología, Ingeniería y Matemáticas.

Augusta Ada King, condesa de Lovelace fue una matemática y escritora londinense considerada por muchos como la primera programadora del mundo. Hija del poeta romántico Lord Byron, su madre promovió su interés por la lógica y las matemáticas. Su talento hizo que entablara amistad con el matemático británico Charles Babbage. En particular, ha pasado a la historia su trabajo en la Máquina Analítica. En 1953, se publicaron sus notas y se reconoció la máquina analítica, como

Imagen: Google.es

precursora de los ordenadores y sus notas como las primeras que describen un ordenador y un software. El lenguaje de programación Ada, diseñado por el Departamento de Defensa de EE.UU., fue aprobado en 1980 y el manual de referencia lleva el año de su nacimiento, MIL-STD-1815. Actualmente suele utilizarse en entornos donde se requiere gran seguridad y fiabilidad.

Extracto del artículo de María Merino Maestre en:

https://mujeresconciencia.com/2014/09/24/ada-pionera-de-la-era-digital/