EUSKO JAURLARITZA
GOBIERNO VASCO

nº 43
marzo de 2013

Aurrera!

Boletín divulgativo de Innovación y Nuevas Tecnologías

Publicado por el Gabinete Tecnológico
Dirección de Informática y Telecomunicaciones

ÍNDICE

Seguro que muchos de nuestros lectores son un **BYOD** pero todavía no lo saben. Si quieres conocer en qué consiste y cuáles son sus ventajas e inconvenientes… te recomendamos que leas el primer artículo que hemos preparado para este nuevo boletín Aurrera!

Como segundo artículo, volvemos a tratar el tema de la seguridad, pero esta vez sin necesidad de centrarnos en nuevos aparatos o tecnologías a utilizar. Es verdad que muchos consideran que la seguridad es un tema que sólo se debe tratar una vez que se ha diseñado el sistema o la aplicación informática que nos ha solicitado el cliente, es decir, a posteriori. En este artículo que hemos preparado, por el contrario, se presenta un concepto o filosofía denominado "*Privacy by design*" (**Seguridad desde el diseño**), que trata de remarcar precisamente la importancia que tiene (y los beneficios que puede reportar) el incluir los requisitos de seguridad desde el momento mismo en que se comienza cualquier proyecto, es decir, desde las fases de análisis y diseño. Además, cabe destacar que desde Europa se ha realizado una **propuesta de Reglamento General de Protección de Datos** (enero de 2012), la cual contempla la realización de análisis de impacto sobre la privacidad.

En el apartado "*Alboan*" os informamos de un nuevo proyecto informático que va a llevar a cabo el Gobierno Vasco con el apoyo de EJIE. Se trata de la **migración del Puesto Corporativo**. Con este proyecto, que afectará a todas las personas de la Red Corporativa durante 2013, se instalarán el sistema operativo Windows7, los paquetes ofimáticos Office2010 y LibreOffice, así como los navegadores Internet Explorer 9 y Mozilla Firefox.

Dentro de "*Breves*" vamos a hablar, en primer lugar, de nuevas funcionalidades añadidas a los satélites que pertenecen al sistema de navegación por satélite que se está desarrollado por la Unión Europea, denominada GALILEO, consistentes en **servicios de búsqueda y salvamento**; y, en segundo lugar, vamos a sintetizar las características principales de la **quinta generación WIFI**, conocida como IEEE 802.11ac, **nuevo estándar WIFI,** que estará listo a finales de 2013, y que, entre otras cosas, mejora sustancialmente el caudal de datos de las conexiones inalámbricas. Cabe recordar que la primera generación WIFI data del año 1997, y que tenía un caudal de datos (concepto distinto al de velocidad) de 2 Mbps.

¿Te apuntas al BYOD?

Cada día es más habitual que la Alta Dirección y demás personal de las empresas utilice sus propios dispositivos para desarrollar su trabajo. Este hecho ofrece innumerables ventajas tanto al trabajador como a la empresa (mayor comodidad, movilidad...), aunque también tiene algunos inconvenientes que habrá que tener en cuenta.

DICCIONARIO

[1] **BYOD:** son las siglas en inglés de "*Bring Your Own Device*" ("*Trae Tu Propio Dispositivo*", TTD).

BYOD, en resumen, es una política empresarial donde los empleados llevan sus propios dispositivos a su lugar de trabajo para tener acceso a recursos de la empresa, tales como correos electrónicos, bases de datos y archivos, así como datos y aplicaciones personales. También se le conoce como "*Bring your own technology*" (trae tu propia tecnología), lo cual expresa un fenómeno mucho más amplio, ya que cubre al equipo (hardware) y al software.

Como curiosidad, indicar que BYOD se inspira en una estrategia implantada por algunos **hosteleros** de los años 70 que invitaban a sus clientes a llevar su propio vino y pagar sólo por descorcharlo.

Hace tiempo que las infraestructuras informáticas de las empresas "abrieron" sus puertas a los equipos de uso personal de sus empleados, colaboradores y visitas, sobre todo a partir de los años 90 cuando se produjo el auge de los ordenadores portátiles. A partir de ese momento, comenzó a ser habitual conectarse a los sistemas y aplicaciones corporativas desde cualquier ubicación ajena a la red interna, es decir, desde equipos móviles diferentes a los Ordenadores de los puestos de trabajo de la empresa.

NUEVOS CANALES

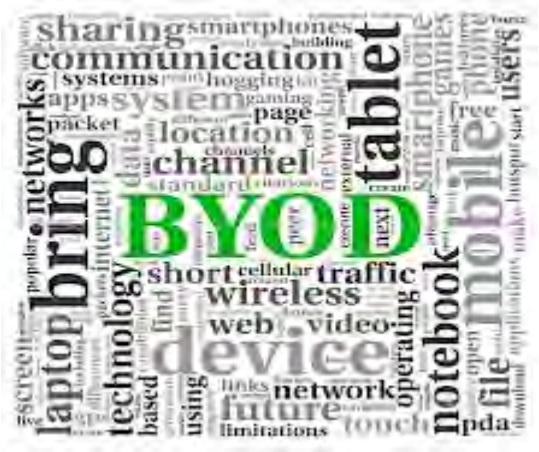
Hasta ahora, el objetivo de las empresas era ofrecer **aplicaciones** y **servicios** que estuviesen disponibles las 24 horas. A partir de ahora, sin embargo, el objetivo será que también estén accesibles desde cualquier **dispositivo**.

Los *smartphones* y *tablets*, que muchos trabajadores compran hoy en día para su uso personal, son capaces de **integrar cualquier aplicación** corporativa. Esto hace que los empleados utilicen el mismo terminal tanto para gestionar sus asuntos personales como laborales, lo que conlleva que muchas empresas se estén planteando cada vez más en serio la estrategia de "trae tu propio dispositivo", tendencia que se conoce con el nombre de BYOD[1].

Esta nueva palabra resume el uso de **dispositivos móviles personales** en el entorno corporativo, donde los propios usuarios (y no la empresa como ocurre hasta ahora) son los que aportan la tecnología.

Si bien muchos opinan que es un riesgo para la empresa, otros muchos expertos consideran que utilizar dispositivos personales como "Puesto de Trabajo" no plantea más riesgos que los que ya tenemos al trabajar con portátiles o memorias USB: riesgo de extravío o pérdida, interceptación de las comunicaciones y/o fuga de información confidencial. En lo que si coinciden todos es en que es necesario aplicar **políticas de seguridad corporativas** sobre los dispositivos que no son propiedad de la organización y sobre los que no se tiene ningún control.

Actualmente, según distintos estudios, empresas de tamaños y sectores muy distintos están siendo requeridas por parte de sus empleados para traer, utilizar y acceder a los recursos corporativos con los dispositivos móviles de su propiedad (básicamente *smartphones* y *tablets)*.

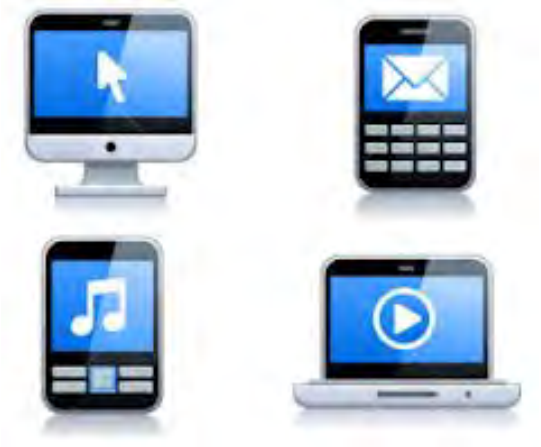


De todas formas, el impacto que pueda tener el BYOD en las organizaciones depende, en gran medida, de las circunstancias particulares de cada organización, y de cómo ha ido gestionando la seguridad corporativa en los últimos años. El BYOD supone un punto de inflexión con respecto a las estrategias tradicionales, donde en la toma de decisiones se buscaba un equilibrio entre el modelo de **negocio y** las necesidades de **seguridad**.

ESTRATEGIA A SEGUIR

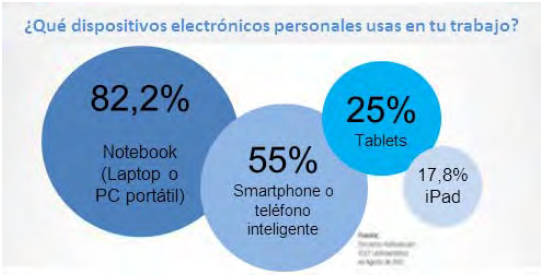
Hasta hace unos años, el funcionamiento habitual

en las empresas era que éstas proveían de equipos a sus empleados (*smartphones*, *notebooks*, etc.) En estos casos, la empresa compraba los equipos (o en algunos casos aplicaba *leasing/renting*, con el consiguiente coste financiero) y no sólo eso, sino que cargaba el software interno, compraba licencias corporativas, cubría seguros de robos, hurtos y desapariciones, asumía el deterioro del mismo o la conocida obsolescencia tecnológica.



Más recientemente, sin embargo, algunas empresas han comenzado a hacer cálculos y han comprobado que mucho dinero que no se recupera viene precisamente de la infraestructura tecnológica de su personal. Por ello, algunas empresas han comenzado a convenir con el empleado a que use su equipo personal (cuyo coste de operación es asumido por la empresa).

Si bien se puede considerar que BYOD es un fenómeno de reciente aparición, éste ya está empezando a provocar grandes cambios en el mundo de los negocios, puesto que alrededor de un 90% de su personal (en los países desarrollados) utiliza sus equipos para acceder a la información de la empresa. Algunos expertos afirman que BYOD ayuda a los empleados a ser más productivos, básicamente porque les ofrece la flexibilidad que necesitan dentro de la empresa.



De todas formas, no todo son ventajas, ya que de no establecer los controles necesarios, esta práctica puede ser perjudicial para la organización: se pueden abrir fisuras por donde se filtre información confidencial o ser la nueva entrada de aplicaciones malignas a la red. Por ejemplo: si un empleado utiliza un *smartphone* para acceder a la red interna de la compañía y luego lo pierde, todos los datos confidenciales guardados en el teléfono podrían llegar a ser accesibles por personas no adecuadas.

ASPECTOS A TENER EN CUENTA

Esta nueva tendencia, como ocurre con cualquier otra tecnología o solución, tiene aspectos tanto positivos como negativos. Repasemos alguno de ellos:

- **Flexibilidad**. Al utilizar sus propios terminales, los empleados pueden tener más opciones para teletrabajar[2] y hacer uso de sus dispositivos en cualquier momento y desde cualquier lugar. Sin embargo, esto requiere que la empresa despliegue nuevas políticas de control de acceso y que disponga de recursos de red suficientes para soportar las conexiones de una mayor cantidad de dispositivos (cada uno con su sistema operativo y sus aplicaciones particulares).
- **Reducción de costes**. Si los dispositivos los aportan los empleados, las empresas se ahorrarían una parte de su inversión en equipamiento (*hardware*). Al mismo tiempo, la empresa suele asumir los servicios de telecomunicaciones, gracias a lo cual los trabajadores no tienen que pagar nada aunque también utilicen los terminales para asuntos personales.
- **Eficiencia**. Los empleados pueden gestionar asuntos urgentes en tiempo real desde cualquier sitio, haciendo uso de sus dispositivos favoritos y conocidos.
- **Productividad**: En general, la principal ventaja que los expertos en TI observan en BYOD es un aumento en la productividad de los empleados, (los usuarios disponen de aplicaciones que usan de forma habitual, lo cual les permite trabajar de forma más cómoda, sin la necesidad de tener que aprender el uso de nuevas aplicaciones, etc.) Este aspecto es importante porque muchos creen que los empleados pueden distraerse con contenidos y aplicaciones personales (p.ej., usando redes sociales, jugando, usando páginas no autorizadas, etc.)

DICCIONARIO

[2] **Teletrabajo:** El Decreto 92/2012, de 29 de mayo, aprueba el Acuerdo sobre la prestación del servicio en la modalidad no presencial (teletrabajo) por el personal de la Administración General de la Comunidad Autónoma de Euskadi y sus Organismos Autónomos.

(BOPV Nº 111, jueves 7 de junio de 2012)

Un aspecto negativo para los empleados es que pueden trabajar más horas de las que les corresponden (muchos están conectados en todo momento, revisando su correo y realizando tareas fuera de su horario laboral)

¿Y LA SEGURIDAD?

Este es un aspecto de máxima importancia.

Las organizaciones que quieran o estén pensando en implementar BYOD deben asegurarse de **proteger** todos los dispositivos que vayan a tener contacto con la información de la empresa. El principal objetivo, por tanto, debe ser evitar cualquier tipo de **fuga de información**. Esta labor, lógicamente, se complica al existir una mayor variedad de equipos a proteger y esto, a su vez, aumenta el costo de la protección.

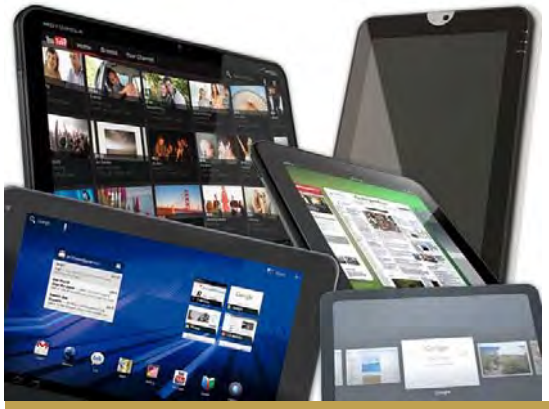
Otro aspecto a tener en cuenta es el futuro de la información en caso de que el usuario deje de trabajar en nuestra empresa, ya que su dispositivo contendrá información de la empresa así como personal. Para evitar este último problema, algunas empresas han optado ya por hacer firmar a los empleados cláusulas de confidencialidad, en las cuales estos ceden toda la información contenida en los dispositivos (incluida la de carácter privado).

"EE.UU. es líder mundial en adopción de BYOD; las empresas asiáticas y latinoamericanas fomentan su uso; mientras que Europa es más cauta."

NUEVOS REQUISITOS

El fenómeno BYOD, en algunos casos, está haciendo que muchas organizaciones se den cuenta que tienen una red inalámbrica *WiFi* un tanto obsoleta que respondía perfectamente a los requisitos de hace unos años, pero no a los actuales.

Está claro que el Departamento más afectado por la entrada de dispositivos móviles personales que, hoy en día, suelen traer los "nativos digitales[3]" a la empresa es el asociado con las TI (Tecnologías de la Información), un área en el que hay que incluir al Responsable de TI, al Director de Sistemas, de Comunicaciones, Asistencia Técnica y/o de Seguridad.



ESTADÍSTICAS

Tal y como podemos comprobar día a día, cada vez más usuarios adquieren dispositivos móviles para uso personal en todo el mundo.

Os incluimos a continuación un resumen de las cifras más significativas sobre la **penetración** de los *smartphones* y *tablets* en 2012:

- ✓ Penetración de los *smartphones*:
  Estados Unidos 44%; Canadá 33%; Reino Unido 51%; Francia 38%; Alemania 29%; Rusia 25% (en 2011); China 33%; India 23% (en 2011); México 20% y Brasil 14%.
  (fuente: *Google/IPSOS*)
- ✓ Penetración de las *tablets*:
  Estados Unidos 42%; Canadá 22%; Reino Unido 28%; Alemania 12%; Francia 19%; Rusia 3%; China 3%; India 2%; México 3% y Brasil 4%.
  (fuente: *Strategy Analytics*).

Centrándonos en **España**, indicar que la gran mayoría de las empresas españolas están interesas en esta nueva tendencia llamada BYOD. Sin embargo, sólo el 18% de ellas ha desarrollado una estrategia sobre cómo implantarla, es más, todavía más de un 40% ni siquiera admite el uso de dispositivos personales en las actividades profesionales.
(fuente: @asLAN)

DICCIONARIO

[3] **Nativos digitales:** Se denomina "nativo digital" u "homo sapiens digital" a todas aquellas personas nacidas durante o con posterioridad a las décadas de los 80 y los 90 del siglo XX, es decir, cuando ya existía la tecnología digital. Por contra, también ha sido acuñado el término "inmigrante digital", haciendo referencia a todo aquel nacido antes de los años 80 y que ha experimentado todo el proceso de cambio de la tecnología.

La incorporación de los **nativos digitales** al mundo laboral ha hecho que BYOD sea una realidad y es el usuario quien elige con qué dispositivo realizar sus comunicaciones. Es más, muchos usuarios, antes que aceptar un *downgrade* y resignarse a una experiencia de usuario incompleta (fruto de unos procesos rígidos de seguridad en la TI), prefieren cargar con dos dispositivos, uno para uso personal y otro para uso profesional.

De todas formas, BYOD no sólo implica al Departamento de TI, sino que afecta también al Departamento financiero, al de Recursos Humanos y también al jurídico, ya que todos ellos deben estar alineados para concretar qué aplicaciones de la compañía se habilitan en el equipo del trabajador, qué datos salen de la empresa, qué permisos se le otorgan, quién usará qué aplicaciones y en qué condiciones económicas, laborales y de horario.

"La incorporación de los «*nativos digitales*» al mundo laboral ha hecho que BYOD sea una realidad y es el usuario el que elige con qué dispositivo realizar sus comunicaciones."

Ante esta nueva tendencia, que poco a poco irá a más (ya que las nuevas generaciones están acostumbradas a usar dispositivos inteligentes en su entorno personal y no quieren renunciar a ellas) las empresas han comenzado a tomar algunas medidas para mejorar la seguridad:

1. Crear **políticas y protocolos** de privacidad y seguridad para acceder a la información. Según muchos expertos, el principal problema de BYOD es que deja el control en manos de los empleados, quienes muchas veces no se preocupan por la seguridad hasta que es demasiado tarde.
2. Usar **aplicaciones web**. De esta manera, tanto los datos como la aplicación residen en un servidor Web seguro, sin dejar nada en el equipo del usuario.
3. Usar **MDM**[4] (*Mobile Device Management*). Esto nos asegura que las políticas de seguridad y conexión se ejecuten en la empresa. (En el mundo del PC mantener una disciplina homogénea es muy fácil, pero no así en el entorno de las *tablet* y *smartphones* donde la gestión es más complicada).

Según estudios recientes, Estados Unidos es líder mundial en política y adopción de BYOD; las empresas asiáticas y latinoamericanas, por su lado, apoyan (y fomentan) un amplio uso de esta nueva filosofía; mientras que Europa es más cauta y restrictiva. [ver en la página anterior el recuadro "*Estadísticas*"]

Antes de acabar, y una vez leído el artículo ¿podrías decirnos ahora si te apuntas al BYOD? ❑

ALGUNOS EJEMPLOS

Estudios recientes indican que existe un número cada vez mayor de profesionales que trabajan de forma remota y que usan sus dispositivos personales.

La empresa tecnológica Cisco Systems, por ejemplo, ha comprobado que su programa BYOD ha crecido un 52% en 12 meses, con empleados que llevan un total de 8.144 iPads y 20.581 iPhones.

La compañía farmacéutica Amerisource-Bergen, por su parte, lanzó recientemente su programa BYOD para dar servicio a unos mil empleados.

La compañía española Cepsa, con el objetivo de dar respuesta a la tendencia BYOD, ha desplegado una red de acceso que proporciona cobertura *wireless* a través de más de 500 puntos de acceso.

A pesar de estos ejemplos, señalar que la mayoría de las empresas están todavía en una etapa muy temprana del BYOD.

A la espera de ver si este año es o no el de la expansión de este fenómeno (tal y como afirman las consultoras), en algunos lugares BYOD ya está traspasando las barreras corporativas y su uso se ha extendido a otros ámbitos, como es el **educativo**. A modo de ejemplo, señalar que los 35 colegios que componen el distrito escolar de Forsyth County (Georgia, Estados Unidos) ya han adoptado esta práctica bajo la denominación de BYOT ("*Bring Your Own Technology*", "Trae tu propia tecnología").

DICCIONARIO

[4] **MDM:** son las siglas en inglés de "*Mobile Device Management*". Se trata de un tipo de **software** que permite asegurar, monitorizar y administrar dispositivos móviles, sin importar el operador de telefonía o proveedor de servicios. La mayoría de las MDM permiten hacer instalación de aplicaciones, localización y rastreo de equipos, sincronización de archivos, reportes de datos y acceso a dispositivos, y todo de forma remota. Este tipo de aplicaciones ha tenido una gran aceptación por parte de las empresas y su crecimiento ha sido realmente vertiginoso, debido en gran parte a la popularidad que han tenido los *Smartphones* dentro de las empresas.

http://es.wikipedia.org/wiki/Mobile_device_management

Seguridad desde el diseño (Privacy by design)

Generalmente, la protección de los Datos de Carácter Personal es vista por los desarrolladores de proyectos, servicios y aplicaciones como un obstáculo y un trámite que se debe cumplir, tomándose en consideración en las últimas fases de los proyectos. "**Privacy by design**" es un nuevo paradigma en este ámbito; trataremos de explicar en qué consiste en las siguientes líneas.

DICCIONARIO

[5] **AVPD:** Agencia Vasca de Protección de Datos; 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.net)

[6] **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.

[7] **PET:** Acrónimo de *Privacy Enhancement Techniques,* tecnologías de protección del derecho a la intimidad. Es un sistema coherente de medidas que protege el derecho a la intimidad suprimiendo o reduciendo los datos personales o evitando el tratamiento innecesario o indeseado de los mismos, sin menoscabo de la funcionalidad de los sistemas de información.

La primera vez que escuché hablar de "***Privacy by design***" fue en mayo de 2011, en la "*euskal securiTIConference*", si bien, ya en 2009, en la 31ª Conferencia Internacional de Protección de Datos y Privacidad (ver a pie de página el cuadro "Medidas Proactivas"), celebrada en Madrid, en la quinta sesión plenaria, se habló de este concepto, lanzándose las siguientes preguntas: *¿en qué momento del diseño de una aplicación debe considerarse la vida privada?, ¿qué metodología debería seguirse?, las referencias normativas existentes ¿son suficientes?, ¿cómo puede influirse en los profesionales? y ¿debe incorporarse el diseño respetuoso con la privacidad a la cultura empresarial?* En la 32ª Conferencia celebrada en Jerusalén, en el año 2010, se firmó una resolución sobre la materia. En aquel congreso vasco sobre la seguridad de la información, organizado por el Colegio Oficial de Ingenieros en Informática del País Vasco y el Departamento de Industria, Innovación, Comercio y Turismo, Pedro Alberto González, responsable del registro de protección de datos y nuevas tecnologías de la Agencia Vasca de Protección de Datos (AVPD[5]), realizó una ponencia bajo el título "*Privacy by design: Construyendo soluciones que garanticen la privacidad desde el primer diseño*" (http://www.slideshare.net/pagonzalez/presentacin-pagonzalez-en-euskalsecuritic), en dicha ponencia subrayó, entre otras cosas, que **la privacidad es un derecho que debe ser incluido de una forma proactiva**, y nos acercó los conceptos de **PIA**[6] (*Privacy Impact Assessment-Evaluaciones de Impacto en la Privacidad*) y **PET**[7] (*Privacy Enhancement Techniques-Tecnologías de Mejora de la Privacidad*).

En lo que respecta a Europa, se ha presentado una **propuesta de Reglamento General de Protección de Datos (enero de 2012)**, la cual contempla la realización de análisis de impacto sobre la privacidad (PIAs), tarea que en las legislaciones sobre protección de datos de algunos países europeos ya se ha introducido como

MEDIDAS PROACTIVAS

La 31ª **Conferencia Internacional de Protección de Datos y Privacidad** elaboró una Resolución denominada "**Estándares Internacionales sobre Protección de Datos Personales y Privacidad**", en la misma hay un capítulo, dentro del apartado **cumplimiento y supervisión,** dedicado a las medidas proactivas, entre las cuales destacamos dos:

- *La adaptación de aquellos sistemas y/o tecnologías de información destinados al tratamiento de datos de carácter personal a la legislación que resulte aplicable en materia de protección de la privacidad en relación con el tratamiento de datos de carácter personal, en particular al decidir acerca de sus especificaciones técnicas y en su desarrollo e implementación.*
- *La puesta en práctica de estudios de impacto sobre la privacidad previos a la implantación de nuevos sistemas y/o tecnologías de información destinados al tratamiento de datos de carácter personal, así como a la puesta en práctica de nuevas modalidades de tratamiento de datos de carácter personal o a la realización de modificaciones sustanciales en tratamientos ya existentes.*

recomendación; este análisis de impacto deberá incluir, entre otras cosas, una evaluación de los riesgos para los derechos y libertades de los interesados.

ORÍGENES

El concepto "*Privacy by design*" fue acuñado a principios de la década de los 90 por la Comisionada de Información y Privacidad de la provincia de Ontario (Canadá), Dra. **Ann Cavoukian**, quien se ha encargado de difundirlo y promocionarlo desde entonces. Este término se refiere a la filosofía y al enfoque para incorporar la privacidad en las especificaciones de diseño de las diferentes tecnologías.

Desde el atentado del 11-S parece que todo está permitido para garantizar la seguridad, dejando en un segundo plano la privacidad de las personas. La idea que remarca la doctora es que no se debe elegir entre seguridad y privacidad (ver en el cuadro inferior el 4º principio fundamental de *Privacy by Design*), esto es, no debemos eliminar la privacidad en aras de una mayor seguridad, sino

LOS 7 PRINCIPIOS FUNDAMENTALES DE PbD[8]

1. **Proactivo, no Reactivo; Preventivo no Correctivo**

Privacy by Design (PbD) se caracteriza por medidas preventivas, no reactivas; anticipa y previene eventos de invasión de privacidad antes de que estos ocurran, no espera a que los riesgos se materialicen, ni ofrece remedios para resolver infracciones de privacidad una vez ocurridas, su fin es prevenirlas, esto es, llegar antes del suceso, no después.

2. **Privacidad como la Configuración Predeterminada (por defecto)**

Lo que manda es lo predeterminado. Que los datos personales estén protegidos de forma automática en cualquier sistema y en cualquier práctica de negocio. El sistema debe estar construido de tal forma que, sin ninguna acción predeterminada, la privacidad esté protegida "*per se*" (lo contrario de lo que ocurre a día de hoy con Facebook).

3. **Privacidad incrustada en el Diseño**

La privacidad se convierte en un componente fundamental de la funcionalidad central que está siendo entregada, es una parte integral del sistema, sin disminuir su funcionalidad, pensada de antemano.

4. **Funcionalidad Total-"Todos ganan", no "Si alguien gana, otro pierde"**

Evita falsas dualidades del tipo privacidad *versus* seguridad, demostrando que sí es posible tener ambas al mismo tiempo, sin tener que recurrir a la frase "si alguien gana, otro pierde".

5. **Seguridad Extremo-a-Extremo. Protección del Ciclo de Vida Completo**

Habiendo sido incrustada en el sistema antes de que el primer elemento de información haya sido recolectado, *Privacy by Design* se extiende con seguridad a través del ciclo de vida completo de los datos involucrados, -las medidas de seguridad robustas son esenciales para la privacidad, de inicio a fin-. Esto garantiza que todos los datos son retenidos con seguridad, y luego destruidos con seguridad al final del proceso, sin demoras. Por lo tanto, PbD garantiza una administración segura del ciclo de vida de la información, desde el inicio hasta el final, desde un extremo hacia el otro.

6. **Visibilidad y Transparencia-Mantenerlo abierto**

PbD busca asegurar a todos los involucrados que cualquiera que sea la práctica de negocios o tecnología involucrada, ésta en realidad está operando de acuerdo a las promesas y objetivos declarados, sujeta a verificación independiente. Sus partes componentes y operaciones permanecen visibles y transparentes, a usuarios y proveedores.

7. **Respeto por la Privacidad de los Usuarios-Mantener un enfoque Centrado en el Usuario**

Por encima de todo, PbD requiere que los arquitectos y operadores mantengan en una posición superior los intereses de las personas; esto es, mantener al usuario en el centro de las prioridades.

Fuente:
http://www.privacybydesign.ca/content/uploads/2009/08/7foundationalprinciples-spanish.pdf
(*Information and Privacy Commissioner of Ontario*)

DICCIONARIO

[8] **PbD:** siglas de *Privacy by Design*, para más información ver: www.privacybydesign.ca

que debemos conservar ambas, entendiendo que la privacidad es la base de muchas de nuestras libertades.

RESOLUCIÓN PBD

Como se ha dicho al principio, "*Privacy by design*" se convirtió en un estándar internacional en la 32ª Conferencia Internacional de Protección de Datos y Privacidad, a través de una resolución, cuyo objetivo es consolidar la privacidad de la información en el futuro.

Hoy en día, cuando nos planteamos el tema de la protección de datos y la privacidad, los responsables de tratamientos miran exclusivamente a la normativa de protección de datos de carácter personal para no caer en su incumplimiento, sin ver la incidencia que tienen los datos recogidos en la privacidad de las personas, por ello se habla de una nueva **filosofía de diseño PbD**[9].

La resolución de "*Privacy by design*" trata de que el concepto "privacidad" se integre en las nuevas tecnologías y organizaciones directamente, desde un principio, como un componente fundamental de la protección de la privacidad, tanto desde el punto de vista técnico como organizativo, es decir, la privacidad incorporada en el diseño de las nuevas tecnologías, prácticas empresariales e infraestructuras, tratando de manera proactiva la privacidad como algo por defecto, en vez de que ésta sea añadida a posteriori, ya que no sólo por cumplir con las regulaciones vigentes se va a garantizar la privacidad.

Las nuevas tecnologías, como todos sabemos, van a una velocidad muy rápida, mucho más rápida que las leyes, por ello es fundamental que estas nuevas tecnologías, así como las organizaciones, adopten este principio de **privacidad por defecto** dentro del análisis inicial de los productos y servicios, como un requisito más, como los requisitos de accesibilidad, seguridad, usabilidad… que hoy en día todo el mundo incorpora desde un principio. Este concepto se está adoptando cada vez más en diferentes organizaciones, siendo proactivo y preventivo.

PBD Y SU TRILOGÍA

Privacy by Design (PbD), si bien en un principio se enfocaba a la tecnología, que era su principal área de actuación, hoy en día se extiende a otras dos áreas o entornos, con lo cual comprende a las tres áreas siguientes:

- ✓ Sistemas TIC (Tecnologías de Información y Comunicaciones)
- ✓ Prácticas de negocio responsables
- ✓ Diseño físico e infraestructura de red

La tecnología en sí no es ninguna amenaza para la privacidad, el problema suele ser la forma en que ésta se utiliza. Los beneficios de adoptar buenas prácticas de privacidad consisten en la obtención de un retorno de la inversión (*ROI*[10]), además de conseguir confianza y mayor satisfacción por parte del cliente. En definitiva, se puede concluir que la privacidad es buena para los negocios.

TECNOLOGÍAS DE VIGILANCIA INVASIVAS

Sabemos que existen tecnologías de vigilancia invasivas que, en la actualidad, se están utilizando de una forma bastante extendida, y que, de una forma u otra, todos "sufrimos", como son las

tecnologías de identificación por radiofrecuencia (RFID[11]), las tecnologías de identificación, vigilancia y control (cámaras de vigilancia públicas y privadas), las tecnologías que utilizan datos biométricos (control de acceso y seguridad), imágenes corporales (escáneres de cuerpo entero), seguimiento de red y monitorización (proveedores de servicios de Internet -ISPs-), sistemas de recopilación de identidades digitales, etc.

A menudo, estos sistemas de seguridad se basan en renunciar a una porción de nuestra privacidad en aras de la seguridad; el principio PbD defiende la introducción de la defensa de los principios de la privacidad desde una primera fase del desarrollo de estos productos y servicios, además, concluye que se pueden incluir sin mermar la seguridad de los datos ni la funcionalidad del sistema. Los riesgos de seguridad de los datos

DICCIONARIO

[9] **Filosofía de diseño PbD:** un diseñador de sistemas/servicios debe partir desde la posición de proteger la privacidad de las personas. Para ello, se hará las estas preguntas: ¿necesito recoger algún dato de carácter personal?, si es que sí, ¿cuál es el mínimo necesario?, ¿quién tendrá acceso a estos datos?, ¿cómo pueden estar estos accesos controlados para que sólo las personas/ procesos autorizados accedan a ellos?...

[10] **ROI:** *return on investments*, retorno ó rendimiento sobre la inversión. Compara el beneficio o la utilidad obtenida en relación a la inversión realizada.

[11] **RFID:** *Radio Frequency Identification*, identificación por radiofrecuencia. RFID se basa en un concepto similar al del sistema de código de barras; la principal diferencia entre ambos reside en que el segundo utiliza señales ópticas para transmitir los datos, y RFID emplea señales de radiofrecuencia (Boletín Aurrera nº42, junio de 2011, artículo "*La tecnología RFID*")

están presentes durante todo su ciclo de vida, por lo que uno de los objetivos es minimizarlos.

Vamos a ver algunos ejemplos de tecnologías orientadas a reforzar la privacidad (PET):

- **Datos biométricos**

En este caso se debe evitar la creación de grandes bases de datos biométricas centralizadas, así mismo, se recomienda el cifrado de los datos biométricos almacenados y en tránsito.

- **Etiquetas RFID**

Para este sistema de vigilancia y control existe una tecnología, denominada "*clipped tag*", desarrollada por IBM, que permite a los consumidores deshabilitar la antena de forma automática, por ejemplo, del modo en que se quitan los sellos de su hoja original (línea de puntos), o rascándolas, como los boletos de lotería.

- **Videovigilancia**

Los datos recogidos por estas tecnologías se visualizan, almacenan, indexan y se guardan. Un uso correcto de los mismos puede servir para prevenir la delincuencia y recoger evidencias, sin embargo existe una clara preocupación acerca de cómo serán utilizadas las imágenes grabadas. Existen tecnologías que cifran los objetos de interés de una grabación (cuerpos y caras), y que sólo serán descifrados en caso de investigación.

- **Imágenes corporales**

Las tecnologías de escaneo de pasajeros empiezan a ser comunes en un gran número de aeropuertos, siendo utilizadas para identificar posibles amenazas de seguridad. El problema es que infieren gravemente en la intimidad de las personas. Por ello, se están utilizando tecnologías que envían las imágenes cifradas a un lugar remoto, donde son exploradas por un empleado que no tiene interacción física con la persona escaneada, no pudiéndose almacenar, enviar ni imprimir, siendo eliminada antes de la siguiente exploración; además se le aplica un filtro de privacidad, por lo que sólo se ven las posibles amenazas, dejando los cuerpos y las caras difuminados.

- **Seguimiento de red y monitorización**

Los proveedores de servicios de Internet recogen gran cantidad de datos de sus usuarios, como, por ejemplo, las actividades en línea de estos, lo cual puede llegar a ser un problema en caso de robo, pérdida o venta. Para combatir esto, la Universidad de Toronto ha creado un sistema denominado "bunker", que permite al proveedor de servicios recopilar datos sensibles y almacenarlos en un sistema a prueba de manipulaciones y que gestiona una serie de informes, de tal modo que un ataque contra él puede llevar a la destrucción de los datos sensibles antes de que el atacante pueda conseguirlos.

- **Identidades digitales**

Internet muchas veces nos obliga a identificarnos digitalmente, el **robo de identidades** (ver recuadro a pie de página) es una lacra que está mermando la confianza del usuario en Internet; además, la unión de estas credenciales pueden aportar perfiles muy concretos de las personas. Para combatir esto existen tecnologías que reducen al mínimo la recogida y uso de los datos personales aportados.

Además de estas herramientas y tecnologías orientadas a reforzar la privacidad, debemos tener en consideración las soluciones y técnicas que incorporen por defecto las opciones de privacidad más restrictivas (*privacy by default*), así como diseñar modelos de metadatos para el intercambio de datos de carácter personal que garanticen el cumplimiento de la normativa, junto con el uso de tecnologías DLP[12] (*Data Loss Prevention*). Otra área donde hay que cuidar la privacidad es en el mundo de las redes sociales, aquí es donde las Agencias de Protección de Datos están informando y formando a los usuarios de estas redes de cómo conseguir un uso responsable de las mismas. ❑

ROBO DE IDENTIDADES

El robo de identidades consiste en que un atacante, por medios informáticos o no, obtiene información personal, y utiliza ésta de forma ilegal. Es el delito de mayor crecimiento en el mundo. Existen diferentes métodos para obtener esa información:

- **Mediante *phishing*[13] y correos falsos**: el atacante se hace pasar por una organización, banco o empresa verdadera.
- **Personal**: a través de información que se escucha y/o ve.
- **Ataque organizado**: intentando romper la seguridad de una empresa, banco u organización para obtener datos de sus clientes. (Fuente: http://es.wikipedia.org)

DICCIONARIO

[12] **DLP:** acrónimo del inglés *Data Loss Prevention,* conjunción de diferentes mecanismos y procedimientos de seguridad cuyo objetivo es evitar las temidas fugas de información sensible o confidencial. (ver Boletín Aurrera nº33, de marzo de 2009, artículo "*Seguridad en dispositivos móviles externos*")

[13] **Phishing:** Del inglés *fishing* «pesca». Hace alusión al acto de "pescar" usuarios mediante señuelos para obtener información secreta sobre ellos. También se dice que es la contracción de «*password harvesting fishing*» (cosecha y pesca de contraseñas). La primera vez que se habló de phishing fue en 1996 y se hizo en el grupo de noticias de hackers "alt.2600". (Ver Boletín Aurrera nº22, de marzo de 2009, artículo "*Ciberdelitos*")

ALBOAN:

Migración al nuevo Puesto Corporativo

"La migración de los 6.000 equipos del Gobierno Vasco se llevará a cabo durante 2013."

Todos sabemos que el mundo de la informática está en constante evolución. Tanto es así que, periódicamente, nos vemos abocados a implantar nuevas aplicaciones o migrar a nuevas versiones los productos que usamos habitualmente. Nuestra organización, el Gobierno Vasco, no es ajena a este tipo de sucesos e históricamente se ha visto obligada a realizar distintas actualizaciones (sistemas operativos, paquetes ofimáticos y otros entornos de *backoffice*).

Pues bien, a lo largo de este año afrontaremos una nueva migración. Por esta razón, y con objeto de explicaros en qué va a consistir exactamente y qué pasos se van a dar, hemos elaborado este artículo.

LOS MOTIVOS

Durante 2012, el Gobierno Vasco inició los preparativos para migrar este año 2013 el Software Base del PC Corporativo. Dicho proyecto, por tanto, afectará a todas las personas que trabajan en la Red Corporativa Administrativa del Gobierno Vasco.

El alcance de este proyecto consiste exactamente en cambiar el PC Corporativo actual (el cual incluye el Sistema Operativo Windows XP, el navegador Internet Explorer 8 y la Suite Ofimática MS Office 2003) y que éste pase a tener como sistema operativo el Windows 7, como navegador de Internet el Explorer 9 y el Mozilla Firefox, y, finalmente, como paquete ofimático el MS Office 2010 y el LibreOffice 3.

Las **razones** por las que se va a realizar la migración son, entre otras, las siguientes:

- Obsolescencia tecnológica: al no poder actualizar los sistemas actuales, dejan de estar protegidos y podrían ocurrir problemas de seguridad graves.
- Soporte de WindowsXP-SP3: en abril de 2014 finaliza el soporte que actualmente dispone el Gobierno Vasco para este sistema operativo.
- Nueva arquitectura: se quiere tener una nueva arquitectura del PC que ofrezca una mayor independencia entre las capas que lo componen (Hardware / Sistema Operativo / Aplicaciones / Datos).
- Funcionalidades: es necesario disponer de mayores funcionalidades (WiFi, USB…).
- Razones económicas: si se quiere ofrecer un mejor servicio, es necesario contar con una mayor automatización y menos procesos manuales (tiempo por reinicios y parcheos) que los sistemas actuales no permiten.

ALCANCE

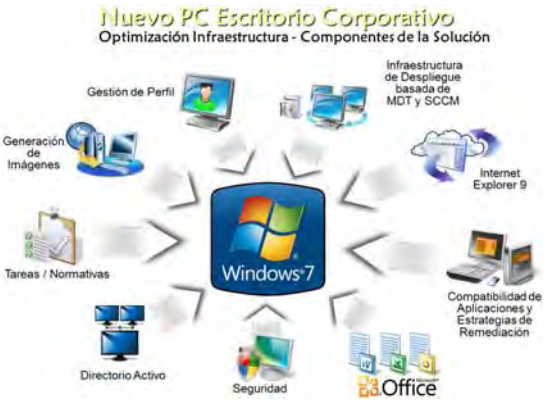
El "diseño" del nuevo PC Corporativo no es una tarea fácil y sencilla, ya que incluye una serie de trabajos previos que el personal técnico de EJIE tiene que llevar a cabo para que el proyecto tenga éxito, o dicho de otra forma, que cause las mínimas molestias posibles a los usuarios finales. Algunas de las tareas que se están realizando son las siguientes:

- ✓ Establecer los **mecanismos** de despliegue necesarios para que la operación de migración sea lo más "transparente" posible
- ✓ Diseñar el proceso de migración de los **datos** del usuario (cuanto mayor sea el volumen de datos a salvar, más tiempo se requerirá)

- ✓ Establecer el nivel de **seguridad** adecuado del equipo (perfiles, configuraciones, etc.)
- ✓ Comprobar la **compatibilidad** de todas las aplicaciones existentes en los Departamentos

El trabajo a realizar se complica un poco más si tenemos en cuenta que el alcance del mismo abarca a todos los Departamentos y Organismos Autónomos del Gobierno Vasco. En este caso, estaríamos hablando de unos 6.000 equipos aproximadamente. Además, tal y como hemos comentado, hay que comprobar la compatibilidad de todas las aplicaciones corporativas existentes (aproximadamente 740, de las cuales 500 son web y 240 Cliente/Servidor); así como chequear el funcionamiento del hardware que se utiliza habitualmente (impresoras, escaners… y demás periféricos).

Otro aspecto a tener en cuenta, y que requerirá una atención especial por parte de EJIE, son las aplicaciones que hacen uso de bases de datos Access, ya que podrían no funcionar adecuadamente con Office2010.



MUCHO MÁS QUE WINDOWS7

Si bien el proyecto gira en torno al sistema operativo Windows7 Enterprise, se va a aprovechar este mismo proyecto para migrar, por un lado, el Directorio Activo actual a Windows Server 2008 R2, y, por otro lado, la infraestructura actual de SMS2003 al nuevo SCCM (*System Center Configuration Manager*).

Otro tema destacable, tal y como hemos comentado, es que junto al paquete ofimático de Microsoft (Office2010) se va a instalar su equivalente en software libre, en concreto la versión 3.5 de **LibreOffice**.

Asimismo, comentar que los usuarios que así lo deseen podrán elegir el "*perfil de Euskera*" (como idioma de trabajo de la interfaz del sistema operativo y del paquete ofimático) de una manera mucho más fácil y cómoda.

PROYECTO PILOTO

Con la idea de conseguir que todo funcione correctamente antes de llevar a cabo la **migración masiva** en todos los ordenadores de la Red Corporativa del Gobierno Vasco, durante los meses de diciembre y enero pasados se ha realizado un Proyecto Piloto en el que han participado alrededor de 60 personas.

A dichas personas (de distintos Departamentos y de diferentes perfiles) se les ha instalado el nuevo Software Base para que realizasen todas las pruebas posibles y notificasen cualquier incidencia que pudiese surgir.

Durante ese periodo, estas personas han contado con el apoyo y soporte de EJIE (a través del CAU) para ir solventando los problemas que iban surgiendo.

Dado que la interfaz (menús y pantallas) de Windows7 y Office2010 cambia significativamente con respecto a la versión actual, comentar que aquellas personas que no conozcan o no hayan trabajado hasta ahora con estos programas, contarán con una serie de pequeñas fichas de concienciación/formación para dar respuesta a aquellas dudas que les puedan surgir en su trabajo diario.

Una vez finalizado dicho periodo (y reportadas todas las incidencias habidas), los Responsables del Proyecto en EJIE están procediendo a analizarlas para evitar que se repitan.

Según la planificación establecida, se prevé llevar a cabo la migración de los 6.000 equipos del Gobierno Vasco (ordenadores de sobremesa y portátiles) durante este año 2013.

Por lo que a lo largo de los próximos meses iremos teniendo noticias de cómo avanza el proyecto. ❑

"Durante los meses de diciembre y enero pasados se ha realizado un Proyecto Piloto con unas 60 personas."

[+info]:

EJIE (Sociedad Informática del Gobierno Vasco - Eusko Jaurlaritzaren Informatika Elkartea):

http://www.ejie.net

¡¡BREVES!!

nº 43

marzo de 2013

Nueva funcionalidad añadida a los satélites GALILEO

En el boletín AURRERA nº 8 (junio 2002) ya se habló del sistema GALILEO, el sistema global de navegación por satélite desarrollado por la Unión Europea, cuyo objetivo, entre otros, es evitar la dependencia actual con respecto a los sistemas GPS (*Global Positioning System*) americano y GLONASS ruso, ambos pertenecientes al ámbito militar.

El sistema de satélites GALILEO proveerá cinco servicios:

1. **Servicio abierto.** Servicio gratuito orientado al público en general. Precisión y disponibilidad superiores a las ofrecidas por GPS.
2. **Servicio para aplicaciones críticas.** Pensado para aplicaciones donde la seguridad es crítica, como, por ejemplo, el transporte aéreo de pasajeros. Esto será posible gracias a la utilización de receptores certificados de doble frecuencia y al alto nivel de integridad ofrecido.
3. **Servicio comercial.** Obviamente no será gratuito, y será requerido por aplicaciones que necesiten más servicios que los ofrecidos por el servicio abierto, agregando dos señales más cifradas.
4. **Servicio público regulado.** Servicio disponible para el uso de aplicaciones gubernamentales. Debe estar operativo en todo momento y bajo cualquier circunstancia.
5. **Servicio de búsqueda y salvamento.** Las mejoras ofertadas son una recepción en tiempo real de los mensajes de socorro desde cualquier punto de la tierra y una precisión con un error de pocos metros.

Para este último servicio la empresa, con sede en Barcelona, MIER Comunicaciones ha fabricado y diseñado los equipos que añadirán la **funcionalidad de búsqueda y rescate** al sistema de navegación europeo. La funcionalidad de los equipos diseñados consiste en recibir señales de socorro de personas en situación de peligro y retransmitirlas a las estaciones receptoras para organizar el rescate.

A día de hoy ya están en órbita cinco satélites (al finalizar el despliegue se dispondrá de treinta).

Quinta generación WIFI

El estándar de conexión inalámbrica **IEEE 802.11n** mejoraba significativamente la velocidad de transmisión de los estándares anteriores, **802.11b** y **802.11g**, con caudales máximos de 54 Mbps, llegando este primero a caudales máximos de 600 Mbps; además, hace uso simultaneo de dos bandas: 2,4 GHz. y 5 GHz; e introduce el concepto MIMO, múltiples entradas y salidas, lo que se llama transmisión espacial, admitiendo en los dispositivos comerciales, dos o tres flujos espaciales. Pues bien, el 802.11n comienza a quedarse atrás con la introducción del nuevo estándar **IEEE 802.11ac**, que se conoce como la **quinta generación WIFI**, el cuál se prevé que esté listo a finales de 2013, si bien, ya se pueden comprar dispositivos que soportan esta nueva tecnología, como, por ejemplo, los adaptadores para redes 802.11ac de la casa ASUS, los PCE-AC66 dual-band, capaces de alcanzar los 1,3 Gbps.

La idea es que todos los estándares 802.11 sean compatibles con los ya existentes, y que difieran únicamente en la capa física (señales eléctricas y cableado).

Otra versión IEEE 802.11, la denominada **IEEE 802.11ad**, será capaz de alcanzar caudales de **varios Gigabits por segundo** sobre la banda de 60 GHz., pero tiene un problema, sólo sirve para **distancias muy cortas** (unos pocos metros), por lo que será un complemento a los estándares 802.11n y 802.11ac.

Última versión de la especificación 802.11ac:

http://www.ieee802.org