EUSKO JAURLARITZA GOBIERNO VASCO

AURRERA!

Nº 71

marzo 2020

Boletín divulgativo de Innovación y Nuevas Tecnologías
Publicado por el Gabinete Tecnológico
Dirección de Tecnologías de la Información y la Comunicación

ÍNDICE

En el primer artículo de este nuevo ejemplar del boletín Aurrera os presentamos una interesante iniciativa, llamada **Identificador Europeo de Legislación** (ELI), que permite acceder online a la legislación que se publica en cualquier país de Europa en un formato normalizado. A lo largo del artículo veremos cómo se ha gestado el proyecto, los pasos que se han dado hasta la fecha y, sobre todo, las ventajas que ofrece.

En el segundo de los artículos, titulado *«Vulnerabilidades en los móviles»*, retomamos uno de los temas que más problemas causan a las personas/ empresas: la **seguridad de los teléfonos móviles**. Si bien estos dispositivos o *smartphones* forman parte desde hace tiempo de nuestras vidas (tanto laborales como personales), seguimos siendo poco conscientes de los peligros que nos acechan «al otro lado» y de las vulnerabilidades que pueden aprovechar los/as hackers para atacar nuestra intimidad y chantajearnos o directamente robarnos nuestro dinero. A lo largo del artículo, repasaremos algunos casos y, como suele ser habitual, os dejaremos también algunas recomendaciones o consejos a seguir.

Continuando con los consejos sobre Windows10 y Office365, en esta ocasión os presentamos los **nuevos documentos y vídeos de ayuda** que tenéis a vuestra disposición en la intranet Jakina para ser consultados cuando os sea necesario.

En la contraportada, una noticia para los/as amantes de la fotografía y de los concursos… Itelazpi ha convocado una nueva edición de su concurso fotográfico #EmakumeaTeknologian (en castellano, *«la mujer en la tecnología»*), que pretende promover la **igualdad entre mujeres y hombres** e impulsar el empoderamiento de las mujeres.

Para acabar, tendremos la ocasión de conocer la vida de la científica recientemente fallecida a los 101 años Katherine Coleman Goble Johnson, una mujer que dedicó su vida a las matemáticas y que, gracias al trabajo realizado en la **NASA**, contribuyó de manera muy importante al éxito de distintas expediciones, entre ellas, el vuelo del Apolo 11 a la Luna en 1969.

Proyecto ELI (Identificador Europeo de Legislación)

ELI es una iniciativa europea que, gracias a la cooperación entre distintas administraciones, nos permite acceder online a la legislación que se publica en cualquier país de Europa en un formato normalizado.

[1] **ELI:** son las siglas en inglés de *«European Legislation Identifier»* (en castellano *«Identificador Europeo de Legislación»*).

Para más información podéis consultar la página web:

https://elidata.es

y la web de la Unión Europea sobre el proyecto:

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

El Identificador Europeo de Legislación, también conocido por sus siglas ELI[1], es una iniciativa adoptada en 2012 por los países y las instituciones de la Unión Europea, que permite acceder online a la legislación que se publica en Internet en un formato normalizado, de manera que pueda **localizarse**, **intercambiarse** y **reutilizarse** independientemente de dónde sea publicado.

Hoy en día hay mucha información legislativa disponible en internet. Sin embargo, la accesibilidad y la interoperabilidad de los sistemas de información de las instituciones nacionales y europeas se ven obstaculizadas muchas veces por las diferencias de los distintos ordenamientos jurídicos nacionales, así como por la incompatibilidad existente entre los sistemas técnicos utilizados para almacenar y presentar la legislación en los sitios web de cada país.

El Identificador Europeo de Legislación, por tanto, tiene por objeto facilitar el acceso, el intercambio y la interconexión de la información jurídica publicada en los sistemas de información jurídica nacionales, europeos y mundiales, para poner en marcha una red de información legal, disponible como conjunto de datos abiertos y susceptibles de reutilización.

LAS VENTAJAS

Las principales ventajas que nos ofrece esta iniciativa son, entre otras, las siguientes:

- **Acceso**: gracias a la optimización del buscador, ELI facilita la localización y el acceso a los datos jurídicos y, de esta forma, se pueden utilizar más.
- **Transparencia**: al mejorar el acceso a la información jurídica, se facilita también el seguimiento del trabajo de las administraciones públicas y se favorece así la rendición de cuentas.
- **Calidad** y **fiabilidad**: ELI ayuda a mejorar la calidad y la fiabilidad de la información jurídica online, ya que usa identificadores permanentes y metadatos estructurados.
- **Interoperabilidad**: se favorece la interoperabilidad entre los sistemas de información estructurando la información de manera normalizada, pero teniendo en cuenta las características específicas de los distintos ordenamientos jurídicos.
- **Costes**: se aumenta la eficacia de los flujos de información y se ahorra tiempo a la hora de publicar la legislación.

- **Servicios**: el acceso a la legislación de manera estructurada facilita la introducción de servicios de valor añadido para las personas que consultan la información.

Desde el punto de vista técnico, ELI se sustenta en **3 pilares** (que también se conocen como «especificaciones técnicas»):

- ✓ Pilar 1: consiste en asignar un **identificador web** (llamado **URI**[2]) a cada documento o recurso legal.
- ✓ Pilar 2: se trata de utilizar los **metadatos** de la ontología[3] ELI predefinida (estos metadatos especifican la manera en la que se describe la información jurídica).
- ✓ Pilar 3: consiste en publicar los metadatos asociados a esa legislación en **formatos abiertos**, lo cual facilita el intercambio y la lectura mecánica. Para ello, se usa JSON (*«JavaScript Object Notation»*, Notación de Objetos de JavaScript) y RDFa (un conjunto de extensiones de XHTML propuestas por el Consorcio W3C) inyectados en el HTML de cada norma.

TRABAJOS DE COORDINACIÓN

El sistema ELI se puso en marcha en **2012** y desde entonces ya ha sido adoptado por varios países europeos (Austria, Bélgica, Dinamarca, España, Finlandia, Francia, Irlanda, Italia, Luxemburgo, Noruega, Portugal, Reino Unido y Serbia) y por la propia Oficina de Publicaciones de la Unión Europea.

El ordenamiento jurídico español es una realidad compleja y plural, integrada por normas que corresponden a distintos niveles territoriales (estatal, autonómico, foral y local). Sin embargo, a pesar de que esas normas forman parte de un sistema y de que se relacionan entre si, a nivel interno se producen diferencias en los sistemas técnicos usados para almacenar y presentar la legislación en las respectivas páginas web, lo que dificulta el acceso a los/as profesionales del Derecho, las empresas y a la ciudadanía en general y hace muy difícil que los sistemas de información legislativa puedan interoperar entre si.

Debido precisamente a la pluralidad del ordenamiento español, la implementación del identificador ELI se ha tenido que realizar de forma coordinada por todas las Administraciones, de acuerdo con la filosofía marcada por el Esquema Nacional de Interoperabilidad (ENI), el cual tiene presentes las recomendaciones de la Unión Europea.

Por ello, la **Comisión Sectorial de Administración Electrónica** (el órgano técnico encargado de la cooperación de la Administración General del Estado, de las administraciones de las Comunidades

[2] **URI:** son las siglas de *«identificador de recursos uniforme»* (en inglés, *«Uniform Resource Identifier»*) y es una cadena de caracteres que identifica los recursos de una red de forma unívoca.

La diferencia con respecto a un localizador de recursos uniforme (más conocido como URL) es que estos últimos hacen referencia a recursos que, de forma general, pueden variar en el tiempo.

[Fuente: Wikipedia]

[3] **Ontología:** la ontología ELI es un modelo de descripción de los recursos legales, orientado a favorecer su enlace con otros recursos legales, así como su publicación y reutilización.

La ontología de ELI se basa en el modelo de datos establecido en los *«Requisitos funcionales de los registros bibliográficos»* (FRBR, http://archive.ifla.org/VII/s13/frbr/frbr-es.pdf), adaptándose a otras iniciativas actuales de normalización en este ámbito.

DIARIOS OFICIALES

Boletín Oficial del País Vasco (EHAA/BOPV):
http://euskadi.eus/bopv

Boletín Oficial del Territorio Histórico de Araba (ALHAO/BOTHA):
https://www.araba.eus/botha

Boletín Oficial de Bizkaia (BAO/BOB):
http://apps.bizkaia.eus/BT00/BAO_BOB

Boletín Oficial de Gipuzkoa (GAO/BOG):
https://egoitza.gipuzkoa.eus/es/bog

Boletín Oficial del Estado (BOE):
https://www.boe.es

Diario Oficial de la Unión Europea (DOUE):
https://eur-lex.europa.eu

Autónomas y de las entidades que integran la Administración Local en materia de administración electrónica) creó en 2017 un Grupo de Trabajo para estudiar la mejor forma de aplicar el estándar ELI a la legislación española.

A partir del trabajo realizado por este Grupo, la Comisión Sectorial aprobó en

marzo de 2018 la *«Especificación técnica para la implementación del Identificador Europeo de Legislación en España (fase1)»*.

Mediante esta especificación se han establecido las **directrices comunes** que requiere implementar ELI en el contexto español.

En España, finalmente, se ha optado por realizar la implementación en varias fases: en la primera de ellas ELI se aplicará únicamente a la normativa del Estado y de las Comunidades Autónomas. [La complejidad de la normativa local y la variable situación tecnológica de los boletines oficiales de la provincia y de las corporaciones locales han aconsejado implementar ELI a la normativa local en una segunda fase]

Para ello se fijaron las siguientes fechas:

- Antes de **2019** -> implementación por parte del Estado
- Antes de **2020** -> implementación por parte de las Comunidades Autónomas

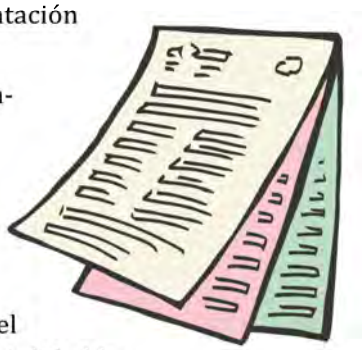
Señalar que en 2018 el Gobierno Vasco se convirtió en la primera Administración Pública del Estado en implantar en su totalidad los 3 pilares del proyecto ELI.

Algunos de los aspectos más destacados de la **Especificación Técnica** aprobada por la Comisión Sectorial de Administración Electrónica es que define el ámbito normativo al que atribuir ELI y la plantilla URI para la normativa estatal y autonómica (Pilar 1), así como un conjunto de metadatos mínimos comunes (Pilar 2).

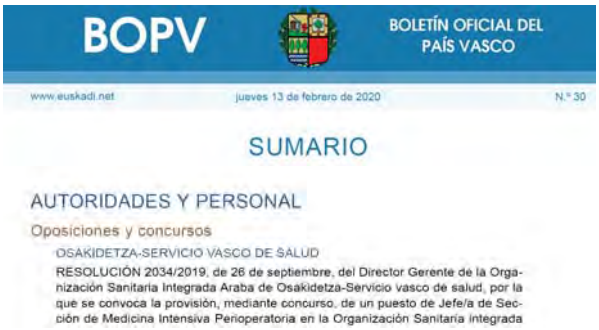
1. **Ámbito de aplicación**: teniendo en cuenta que la mayor parte de la normativa vigente ha sido dictada con posterioridad a la Constitución y que los primeros Estatutos de Autonomía se aprobaron en 1979, el ELI se aplicará al menos, a la legislación estatal y autonómica publicada a partir del 29 de diciembre de 1978. [En el ámbito estatal también se aplicará a todas aquellas normas publicadas con anterioridad y que cuenten con versión consolidada]

«La implantación de ELI es una forma segura y fiable de avanzar en la normalización de los datos abiertos»

2. **Plantilla URI**: se define la estructura de la dirección URI para las normas estatales y autonómicas, que será la siguiente:
/eli/{jurisdiction}/{type}/{year}/{month}/{day}/{naturalidentifier}/{version}/{pointintime}/{language}/{format}



3. **Metadatos comunes**: la implantación de la plantilla URI en España exige que se normalicen los metadatos que utilizan las distintas Administraciones para describir la legislación, al menos aquellos que contienen la información de los componentes de la URI. Por ello, en la primera fase de


BOPV BOLETÍN OFICIAL DEL PAÍS VASCO
www.euskadi.net jueves 13 de febrero de 2020 N.º 30
SUMARIO
AUTORIDADES Y PERSONAL
Oposiciones y concursos
OSAKIDETZA-SERVICIO VASCO DE SALUD
RESOLUCIÓN 2034/2019, de 26 de septiembre, del Director Gerente de la Organización Sanitaria Integrada Araba de Osakidetza-Servicio vasco de salud, por la que se convoca la provisión, mediante concurso, de un puesto de Jefe/a de Sección de Medicina Intensiva Perioperatoria en la Organización Sanitaria Integrada

implementación de ELI en España, el Pilar 1 se aborda conjuntamente con el Pilar 2, para poder establecer una relación de metadatos mínimos comunes que facilite la interoperabilidad de la información legislativa. [La Especificación Técnica prevé una serie de metadatos mínimos comunes]

EL GOBIERNO VASCO

En el caso del Gobierno Vasco, el proyecto para la implantación de ELI ha sido impulsado por la Dirección de Atención a la Ciudadanía e Innovación y Mejora de la Administración (DACIMA).

Las principales características del proyecto han sido las siguientes:

- Normativa publicada en el **BOPV**: se ha implantado el indicador ELI en los contenidos normativos provenientes del Boletín Oficial del País Vasco (BOPV). Cada vez que se publica una norma en el BOPV, se publica también en el área de normativa de **Legegunea**[4] con las especificaciones técnicas de ELI. Esto es posible gracias a un proceso de carga automático (que se realiza diariamente) desde el propio Boletín al portal de Legegunea.
- Legislación desde **1936**: si bien en España se ha establecido la obligatoriedad de aplicar ELI a aquellas normas publicadas a partir del 29 de diciembre de 1978, el Gobierno Vasco lo ha implantado en todas aquellas normas publicadas desde 1936.
- **Normas**: a día de hoy son en total más de 36.000 contenidos normativos de aplicación en Euskadi los que se han integrado en la especificación ELI.

Cada contenido normativo que se publica en Legegunea contiene sus metadatos en formatos reutilizables y semánticos, para lo cual se utiliza JSON y RDFa inyectados en el HTML de cada norma.

Gracias al trabajo realizado, cada uno de los contenidos normativos publicado es accesible mediante una URI que cumple el patrón establecido en ELI y que, como hemos indicado anteriormente, tiene la siguiente forma:

/eli/{jurisdiction}/{type}/{year}/
{month}/{day}/{naturalidentifier}/
{version}/{pointintime}/{language}/
{format}

Ejemplos:

Un recurso legal del Gobierno Vasco tendrá la siguiente estructura:

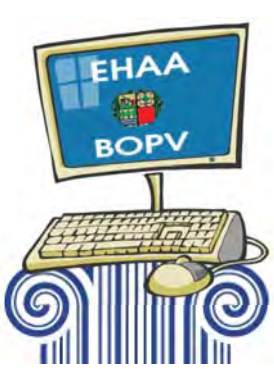
http://id.euskadi.eus/eli/es-pv/
res/2018/12/10/(8)/dof/

Estructura de ese mismo recurso legal en euskera:

http://id.euskadi.eus/eli/es-pv/
res/2018/12/18/(7)/dof/eus/

Las URIs son únicas, es decir, cada recurso legal dispone de un solo identificador web, y además, las URIs son persistentes y, por tanto, no pueden ser eliminadas y en su lugar deben implementarse redireccionamientos.

En definitiva, la implantación de ELI es una forma segura y fiable de avanzar en la normalización de los datos abiertos. ❑



[4] **Legegunea:** es un proyecto del Gobierno Vasco que agrupa en una única web todos aquellos contenidos normativos del ámbito competencial vasco que emanan de nuestro sistema de autogobierno y aquéllos otros, del ámbito estatal, que habilitan éstos o son de aplicación, así como información de relevancia jurídica para entender e interpretar la legislación de Euskadi y conocer ciertos actos y actividades administrativas del propio Gobierno Vasco, y los pone a disposición de la ciudadanía de una forma ordenada y con accesos sencillos y claros.

www.legegunea.euskadi.eus

Vulnerabilidades en los móviles

En este artículo mostraremos algunas recomendaciones para hacer frente a algunos ataques e intrusismos que se han detectado recientemente, y cuyos ataques los han sufrido tanto dispositivos móviles como algunas aplicaciones de uso muy extendido.

[5] ***«Juice Jacking»***: el término fue acuñado por el experto en seguridad Brian Krebs en 2011. Su significado en castellano es «ataque de carga» y tras ese nombre se conoce la amenaza que esconden los puertos USB públicos de recarga de baterías.

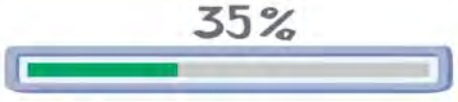
Hoy en día existen en el mercado dos sistemas operativos predominantes: iOS de Apple y Android de Google. Si bien cada uno de ellos tiene su propia idiosincrasia, ninguno de ellos se libra de un mal que cada vez tiene más auge: el ataque de la delincuencia para obtener la información almacenada en ellos.

Estos ataques pueden venir tanto desde el acceso por las características de cada uno de ellos, como por las aplicaciones que tienen instaladas. Repasamos a continuación alguna de las vulnerabilidades detectadas recientemente y, a continuación, daremos algunas recomendaciones que nos permita crear una configuración segura en nuestros dispositivos (principalmente con el sistema operativo iOS pero que bien puede extenderse a otros sistemas).

EL JUICE JACKING

El *«Juice Jacking»*[5] consiste básicamente en la instalación de un *malware* (software malicioso) en nuestro móvil a través del cable USB.

Aunque las baterías tienen cada vez más capacidad, suele ser habitual el tener que recargar el teléfono en algún momento del día (debido a la utilización de más aplicaciones y con mayor frecuencia). Un recurso habitual para muchas personas es recurrir a los puntos de carga USB que hay en lugares públicos (autobuses, etc.) cuando la batería está a punto de agotarse o incluso cuando el propietario del teléfono sufre *«el Síndrome de Batería Baja»* (SBB), que consiste en sentir ansiedad por miedo a que el móvil se apague.



Estos puntos de carga públicos nos ayudan a seguir comunicados y conectados con el resto del mundo, pero hay que ser precavidos/as ya que aprovechar estas conexiones de carga puede traer aparejado un gran peligro para el contenido que tenemos almacenado en nuestro teléfono; en concreto, para la obtención de datos personales que almacena en su interior o, directamente, para el propio dispositivo al instalarse *malware* en el móvil, lo que le puede permitir a un/a hacker, por ejemplo, acceder al teléfono, aunque no esté conectado. Con dicho software, un/a delincuente puede conocer, por ejemplo, las contraseñas que tengamos almacenadas en nuestro dispositivo, información como la dirección de la persona propietaria o su DNI; incluso dejar el teléfono inutilizable.

«Hoy en día, el robo de información puede ser realmente grave teniendo en cuenta, por ejemplo, que las aplicaciones del móvil cada vez se utilizan más para acceder a las cuentas bancarias»

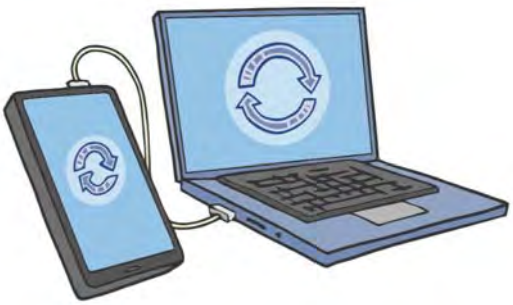
Según distintos estudios, el nivel de riesgo de conectar nuestro teléfono a un puerto de carga USB en un lugar público es similar a

conectarse a una red WiFi pública. Un aspecto en el que fijarse es cuando el punto de carga tiene ya conectado un cable USB (aquellos que incluyen *malware* no se distinguen externamente de un cable USB normal). Pero el riesgo puede residir también en el puerto USB, ya que un/a ciberdelincuente puede sustituir uno normal por otro que contenga código malicioso. Una buena medida preventiva contra este tipo de ataques es indicar en el móvil la opción de sólo recargar y no la opción de transferir datos.

El robo de información puede ser realmente grave teniendo en cuenta, por ejemplo, que las aplicaciones del móvil cada vez se utilizan más para acceder a las cuentas bancarias, de forma que, si los/as delincuentes se hacen con la información almacenada en nuestro dispositivo, podrían entrar al banco y operar directamente con nuestro dinero.

Os pasamos, a continuación, algunas recomendaciones a tener en cuenta para minimizar el riesgo de que nos roben datos de nuestro móvil mediante esta técnica:

- ✓ Llevar siempre una batería recargable portátil llena (en inglés, *«powerbank»*) o el cargador con el enchufe a la red eléctrica, de forma que se pueda enchufar el teléfono directamente a la electricidad y evitar la transferencia de datos.
- ✓ Utilizar solo puertos USB de confianza. No lo son, por ejemplo, los cargadores USB que incluyen los coches de alquiler.
- ✓ Proteger el móvil con contraseña y no desbloquearlo mientras se está cargando.
- ✓ Utilizar un antivirus en el teléfono.
- ✓ Si fuese necesario utilizar un punto de recarga público, apagar el teléfono mientras está conectado. Si es necesario que esté encendido, no desbloquearlo en ningún momento hasta que se haya desconectado.



- ✓ Utilizar unos protectores especiales que existen en el mercado y que deshabilitan el *pin* de intercambio de datos cuando el teléfono se recarga mediante USB, y sólo permite el paso de la corriente eléctrica.
- ✓ Utilizar para la recarga un cable USB sin capacidad de datos, aunque esta opción implica llevar ese cable adicional.

En definitiva, se recomienda no recargar el dispositivo móvil mediante los USBs ubicados en lugares públicos, sencillamente porque nos pueden instalar un malware y robar información directamente desde el dispositivo.

VULNERABILIDAD EN WHATSAPP

Recientemente se ha detectado una vulnerabilidad en Whatsapp (con un nivel de criticidad alto) que empieza con el envío al usuario/a de un archivo MP4.

Esta vulnerabilidad provoca un posible desbordamiento del *«búfer»*, lo que puede provocar ataques de denegación de servicio (DoS[6]) o ejecución remota de código (RCE), es decir, se basan en la sobrecarga de los

[6] **DoS:** son las siglas en inglés de *«Denial of Service»*. Se trata de un ataque a un sistema de ordenadores o una red que provoca que un servicio o recurso sea inaccesible para las personas que quieran hacer uso de él.

Los ataques DoS se generan mediante la saturación de los puertos con múltiples flujos de información, haciendo que el servidor se sobrecargue y no pueda seguir prestando su servicio. Por eso se le denomina denegación, pues hace que el servidor no pueda atender la enorme cantidad de solicitudes que le llegan. Esta técnica es usada por los/as *«crackers»* (piratas informáticos) para dejar fuera de servicio algunos servidores que quieren atacar.

[Fuente: Wikipedia]

sistemas de las víctimas para que el dispositivo o la red de las mismas deje de estar disponible y poder acceder así al robo de su información personal.

Como hemos comentado, se trata de una vulnerabilidad que puede hacerse de forma remota, lo que le hace muy peligroso. Por el momento no se ha detectado la presencia de *«exploits»*[7] públicos disponibles para su descarga que permitan a los atacantes aprovechar esta vulnerabilidad ni actividad en la red relacionada con la misma.

Según Whatsapp, las versiones de aplicaciones afectadas son las siguientes:

- Android: versiones anteriores a la 2.19.274
- iOS: versiones anteriores a la 2.19.100

Esta vulnerabilidad ya ha sido corregida por Whatsapp en las versiones posteriores. Dichas versiones están disponibles

directamente a través de las plataformas de apps correspondientes para cada sistema operativo afectado, como Google Play, App Store de Apple, Microsoft Store, o bien directamente desde la página oficial de Whatsapp: https://www.whatsapp.com

Por lo que se recomienda actualizar la aplicación cuanto antes, ya que el impacto de un ataque exitoso de esta vulnerabilidad puede tener graves consecuencias para nuestra privacidad. Asimismo, se recomienda deshabilitar las descargas automáticas de imágenes, archivos de audio y vídeo desde la configuración de la propia aplicación.

VULNERABILIDADES EN IOS

Recientemente, el fabricante Apple ha lanzado varias actualizaciones que corrigen una serie de vulnerabilidades que afectan a los sistemas macOS, iOS, iPadOS y Safari. Por

el momento no se conocen los detalles exactos de estas vulnerabilidades, pero se ha sabido que algunas de ellas consisten en:

- Un problema con la pantalla de bloqueo puede permitir el acceso a los contactos en un dispositivo bloqueado. En este caso, el problema se ha solucionado mejorando la gestión de los «estados» del sistema operativo.
- Los usuarios eliminados de una conversación de iMessage aún pueden alterar el estado de la misma. Para evitarlo se han mejorado los controles de la aplicación.
- El procesamiento de una imagen creada con fines malintencionados puede provocar la ejecución de código arbitrario. Se han corregido las lecturas fuera de límites con validaciones de entrada mejoradas.
- Las capturas de pantalla de la aplicación Mensajes pueden revelar contenido adicional del mensaje, debido a una emisión en el nombramiento de capturas de pantalla. El problema se ha corregido usando nombres mejorados.
- Problema de validación que puede provocar que una aplicación lea memoria restringida.

De momento, la base de datos del NIST[8] no ha registrado las vulnerabilidades y, por tanto, no ha llevado a cabo el correspondiente análisis. De todas formas, se les atribuye una criticidad alta.

En este caso, los dispositivos afectados son:

- iPhone 6S y posteriores

[7] **Exploits**: es una palabra inglesa que significa explotar o aprovechar. En el ámbito de la informática es un fragmento de software, fragmento de datos o secuencia de comandos o acciones, usada para aprovechar una vulnerabilidad de seguridad de un sistema de información para conseguir un comportamiento no deseado del mismo.
[Fuente: Wikipedia]

[8] **NIST**: son las siglas de *«National Institute of Standards and Technology»* (en castellano, *«Instituto Nacional de Estándares y Tecnología»*).
Es una agencia de la Administración de Tecnología del Departamento de Comercio de los Estados Unidos.
La misión de este instituto es promover la innovación y la competencia industrial en Estados Unidos mediante avances en metrología, normas y tecnología de forma que mejoren la estabilidad económica y la calidad de vida.
Página web:
https://www.nist.gov
[Fuente: Wikipedia]

- iPad Air 2 y posteriores
- iPad mini 4 y posteriores

Apple ha publicado recientemente las correspondientes actualizaciones para todos los dispositivos y versiones afectadas por estos errores. La descarga de las actualizaciones se encuentra disponible en el siguiente enlace:

https://support.apple.com/es-es/HT201222

Se recomienda también actualizar a las versiones más recientes de los sistemas Apple.

[ver cuadro *«Buenas prácticas»*]

Cuidad vuestro móvil. ❑

«Se recomienda no recargar el dispositivo móvil mediante los USBs ubicados en lugares públicos»

BUENAS PRÁCTICAS

Con el siguiente **decálogo** de Buenas Prácticas en Dispositivos móviles se profundiza en la seguridad de nuestros dispositivos, aumentando, de esta forma, el nivel de protección y de seguridad.

Las 10 recomendaciones para mejorar la seguridad son:

1. Fijar un código robusto de acceso al dispositivo (se recomienda que la longitud de la clave de acceso sea de 8 caracteres como mínimo).
2. Mantener las aplicaciones y el sistema operativo actualizado.
3. Hacer uso de la funcionalidad «Restricciones» (en el caso de Apple) para limitar modificaciones en el código de acceso, cambios en la cuenta de iCloud, así como otra serie de permisos.
4. Evitar la conexión a redes WiFi abiertas.
5. Limitar el acceso a la información en la pantalla de bloqueo, deshabilitando el Centro de Control, el acceso al asistente de voz (Siri, Cortana…) y el Centro de Notificaciones.
6. Establecer el bloqueo automático de la pantalla.
7. Desinstalar aquellas aplicaciones que no se estén utilizando.
8. Desactivar los interfaces de WiFi, bluetooth y AirDrop[9] cuando no se estén utilizando.
9. Limitar los permisos otorgados a las aplicaciones (localización, micrófono, contactos, etc.).
10. Proteger la cuenta de usuario/a mediante una contraseña robusta y exclusiva, y habilitar el segundo factor de autenticación.

Por otro lado, podéis consultar la **Guía** de recomendaciones del Gobierno Vasco para un uso más seguro de los dispositivos móviles[10].

[9] **AirDrop:** es el servicio del sistema operativo iOS de Apple que permite la transferencia de archivos entre dispositivos compatibles iOS a través de Wi-Fi y bluetooth sin necesidad de usar correo o un dispositivo de almacenamiento.

[10] **Guía de recomendaciones del Gobierno Vasco:** podéis consultar el documento elaborado por la Dirección de Informática y Telecomunicaciones a principios de 2014 titulado *«Recomendaciones para un uso SEGURO de los dispositivos y de las redes sociales en el Gobierno Vasco»*, el cual recoge mediante distintas ilustraciones los principios básicos a tener en cuenta.

Dicho documento está accesible en la web http://www.euskadi.eus/informatica + apartado *«Seguridad informática»*

ALBOAN:

Consejos sobre Windows10 y Office365: píldoras formativas y vídeos explicativos

«Esta documentación de ayuda está a vuestra disposición en la intranet Jakina, en el apartado "Formación" + "Windows 10 y Office 365"»

Continuando con los consejos sobre Windows10 y Office365 que iniciamos el año pasado, en esta ocasión os queremos presentar una parte de la ayuda que tenéis a vuestra disposición para ser consultada cuando os sea necesario.

Se trata, en concreto, de una serie de vídeos y pequeñas guías que explican cómo hacer algunas tareas o cómo usar algunas funcionalidades del nuevo Windows10 y del Office365.

DOCUMENTOS Y VÍDEOS DE AYUDA

Dado que la nueva plataforma ofrece muchas novedades, la Dirección de Informática y Telecomunicaciones, junto con EJIE, ha decidido publicar una serie de guías o *«píldoras formativas»* para facilitar el uso de las nuevas herramientas por parte del personal del Gobierno Vasco.

Los temas están agrupados en tres grandes categorías (Windows10, Office2016 y Office365) y el contenido de los mismos se ha

dividido de la siguiente forma:

- **Windows10**
- **Office2016**
  - ✓ La aplicación Excel
  - ✓ La aplicación Word
  - ✓ La aplicación Outlook
  - ✓ La aplicación PowerPoint
- **Office365**:
  - ✓ Aspectos de uso general
  - ✓ Características de los Grupos
  - ✓ Funcionamiento de OneDrive
  - ✓ Correo de Outlook
  - ✓ Características de los sitios de Sharepoints
  - ✓ Comunicaciones mediante Skype
  - ✓ Trabajar en equipo mediante Teams

Tal y como hemos indicado, los documentos elaborados son unas pequeñas **guías** o *«píldoras formativas»* que explican de una manera simple cómo se pueden realizar algunas funciones o cómo se usan algunas

funcionalidades del nuevo Word, Excel, etc.

En cuanto a los **vídeos**, estos tienen una duración de 2 minutos aproximadamente y

mediante una serie de ejemplos explican cómo realizar algunas de las tareas más habituales, pudiendo de esta forma sacar un mayor provecho a las nuevas herramientas que ya disponemos en nuestros ordenadores.

[ver cuadro *«Algunos ejemplos»*]

Toda esta documentación está disponible en la intranet Jakina, en el apartado *«Formación»* + *«Windows 10 y Office 365»*. Echadle un vistazo.

«Se ha decidido publicar una serie de guías o "píldoras formativas" para facilitar el uso de las nuevas herramientas a todo el personal del Gobierno Vasco»

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

ALGUNOS EJEMPLOS

En **Windows10** y en **Office365**... – Novedades en Windows10 – Cómo usar el nuevo portapapeles – Cómo instalar Office ProPlus en nuestros dispositivos – Cómo quitar datos personales de los archivos	En **OneDrive**... – Cómo instalar y configurar el cliente de sincronización – Cómo averiguar qué ficheros tengo compartidos – Cómo trabajar con los documentos almacenados en la nube
En **Outlook**... – Cómo gestionar contactos – Cómo crear respuestas automáticas – Cómo configurar la cuenta de correo en Android	En **Sharepoint**... – Cómo invitar a un colaborador externo – Cómo cargar datos – Cómo dejar de sincronizar una carpeta
En **Word**... – Cómo aplicar estilos y temas en Word – Cómo configurar el corrector ortográfico en otro idioma	En **Grupos**... – Cómo crear en O365 un nuevo Grupo – Cómo trabajar con los documentos almacenados en la nube en O365 – Cómo compartir ficheros
En **Excel**... – Cómo trabajar con una tabla dinámica – Cómo crear en Excel listas personalizadas	En **Teams**... – Cómo crear equipos – Cómo utilizar la coautoría-edición simultánea – Cómo crear una reunión
En **PowerPoint**... – Cómo organizar las diapositivas – Cómo grabar en PowerPoint la pantalla	En **Skype**... – Cómo convocar reuniones – Cómo añadir nuevos asistentes una vez iniciada una reunión

ALBOAN

¡¡Contraportada!!

Nº 71

marzo 2020

AL CIERRE

Concurso fotográfico de Itelazpi #EmakumeaTeknologian

Como muestra de apoyo al *«Día de la Mujer y de la Niña en la Tecnología»*, que se celebra el 11 de febrero, Itelazpi ha puesto en marcha la **3ª edición** del concurso fotográfico *#EmakumeaTeknologian* (en castellano, *«la mujer en la tecnología»*).

El concurso tiene como objetivo promover la igualdad entre mujeres y hombres e impulsar el empoderamiento de las mujeres y las niñas.

Según se recoge en las bases publicadas del concurso, pueden participar mujeres y hombres mayores de 18 años.

Así que si conocéis en vuestro entorno alguna mujer que desarrolle estudios y/o trabaje en el sector de la ciencia y la tecnología, podéis enviar a Itelazpi antes del **30 de junio** una fotografía en la que esté realizando su actividad técnica habitual, incorporando además un guiño a la igualdad entre mujeres y hombres. Asimismo, deberéis completar vuestra propuesta con un **título** inspirador y una breve **descripción** de las labores que se muestran en la imagen.

La fotografía que mejor refleje el espíritu del concurso (estilo y mensaje) obtendrá distintos premios, y además aparecerá en la portada del calendario de mesa 2021 que publicará Itelazpi (el cual se completará con otras 11 fotos finalistas).

El 25 de noviembre, con motivo del *«Día Internacional contra la Violencia de Género»*, Itelazpi presentará el calendario completo.

Más información en:
http://www.itelazpi.eus

PROTAGONISTAS

Katherine Johnson, la matemática de la NASA

Katherine Coleman Goble Johnson (Virginia; 26/ago./1918 - Virginia; 24/feb./2020), fue una física y matemática estadounidense que contribuyó a la aeronáutica de los Estados Unidos y sus programas espaciales con la aplicación de las computadoras electrónicas digitales en la NASA.

Desde muy pequeña, Coleman demostró un gran talento para las matemáticas. Sus padres consideraban muy importante la educación de sus hijos/as. Debido a que en el Condado de Greenbrier no se ofrecía escolarización para niñas/os negros más allá del octavo grado, tuvo que asistir al secundario en la comunidad de Institute.

A los 15 años ingresó en la Universidad Estatal de Virginia Occidental. En 1937, con 18 años, se graduó *summa cum laude* , en matemáticas y francés.

En 1938, Coleman Goble Johnson fue la primera mujer afroamericana en terminar con la **segregación** en la Universidad de Virginia Occidental. Fue una de las tres personas afroamericanas, y la única mujer, seleccionada para realizar estudios de posgrado después de una sentencia de la Corte Suprema de los Estados Unidos.

En 1953, le ofrecieron un puesto en la **NASA** que aceptó de inmediato. En su nuevo puesto, Coleman calculó la trayectoria del vuelo espacial de Alan Shepard, el primer estadounidense en viajar al espacio, en 1961. Asimismo, calculó el lanzamiento del Proyecto Mercury de 1961. En 1962, cuando la NASA comenzó a utilizar computadoras electrónicas para calcular la órbita de John Glenn alrededor de la Tierra, fue convocada para verificar los resultados de la computadora. Su capacidad y reputación por la exactitud de sus cálculos ayudaron a confiar en la nueva tecnología. Finalmente, en 1969, fue también la encargada de calcular la trayectoria del vuelo del Apolo 11 a la **Luna**.

En 2016, su vida fue llevada al cine en la película *«Hidden Figures»* (*«Figuras ocultas»*).

Más información en:
https://es.wikipedia.org/wiki/Katherine_Johnson