EUSKO JAURLARITZA GOBIERNO VASCO

AURRERA!

Nº 66

diciembre 2018

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

ÍNDICE

En este nuevo ejemplar os presentamos un nuevo concepto que se hace llamar *«**DevOps**»*. Como veremos a lo largo del primer tema que le hemos dedicado, en realidad no es una metodología de trabajo nueva, pero es ahora cuando parece que empieza a despegar dentro de las grandes organizaciones, gracias a la flexibilidad que ofrece a las empresas a la hora de entregar a sus clientes los productos software (aplicaciones) que desarrollan.

Por otro lado, cuenta la leyenda que los viejos rockeros nunca mueren… y podríamos añadir que muchos de los viejos métodos usados por los hackers para conseguir información y estafar a las personas tampoco, ya que muchos de los métodos de **suplantación de identidades** utilizados desde hace años, siguen campando a sus anchas y provocando grandes perjuicios a las personas (o empresas) que sufren el ataque y no saben defenderse. Por ello, hacemos un breve repaso de algunos de los casos más típicos y, sobre todo, cómo detectarlos y evitarlos. Así mismo, os comentamos qué iniciativas se están llevando a cabo dentro del Gobierno Vasco para concienciar y formar a su personal.

En la sección de *«Alboan»* os presentamos una mejora que se ha incorporado recientemente a la aplicación del **Parque móvil** del Gobierno Vasco, cuyo objetivo principal es reducir el intercambio de papel entre los Departamentos y la Dirección de Recursos Generales. A lo largo del artículo veremos en qué ha consistido.

El intercambiar ideas y experiencias siempre es bueno, y recientemente, el Gobierno Vaco ha tenido ocasión de asistir y participar en el mayor encuentro empresarial sobre Software Libre y Código Abierto, **LibreCon2018**, celebrado en esta ocasión en Bilbao. Os contamos muchos más detalles en el apartado «Al cierre».

En el apartado *«Protagonistas»* repasamos brevemente la vida de **Hedy Lamarr**, una de las grandes inventoras en el ámbito de las telecomunicaciones, así como actriz.

Por cierto,

¡Felicidades y próspero año nuevo 2019!

Así funciona la metodología DevOps

El movimiento DevOps[1] está estrechamente ligado con las metodologías ágiles de desarrollo de software. A lo largo de este artículo repasaremos cuál es su origen, cuáles son sus características, así como las ventajas que ofrece para las grandes organizaciones.

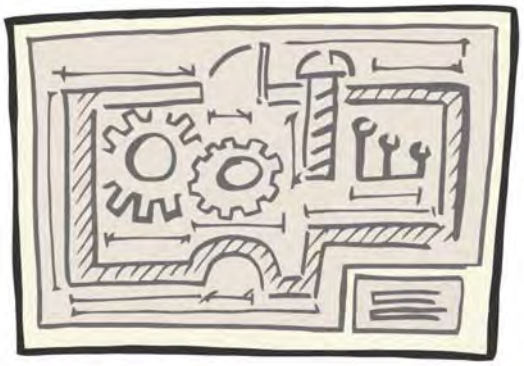
[1] **DevOps**: es el acrónimo inglés de las palabras *development* (desarrollo en castellano) y *operations* (operaciones). Básicamente es una práctica de ingeniería de software que tiene como objetivo unificar el desarrollo de software (Dev) y la operación del software (Ops).

La principal característica del movimiento DevOps es defender la automatización y la monitorización en todos los pasos de la construcción o desarrollo del software, desde la integración, las pruebas, la liberación hasta la implementación y la administración de la infraestructura.

DevOps apunta a ciclos de desarrollo más cortos, mayor frecuencia de implementación, lanzamientos más confiables, en estrecha alineación con los objetivos comerciales.

[Fuente: Wikipedia]

Hasta los años 90 la metodología que se seguía a la hora de desarrollar aplicaciones informáticas era el modelo conocido como «en cascada», que se caracterizaba por tener una serie de pasos muy estructurados y muy estrictos a la hora de ser validados y poder continuar con la siguiente fase, y poder entregar el producto final (programa informático o software) al cliente.



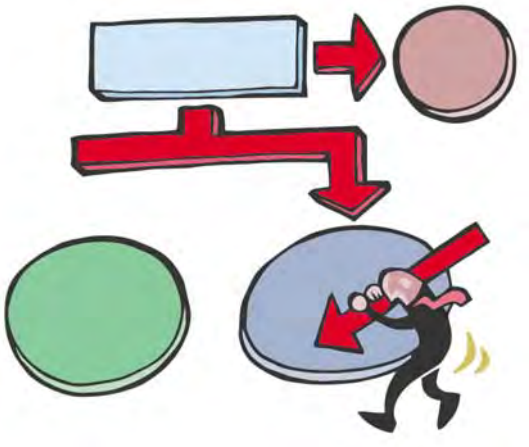
Como respuesta a esta metodología, considerada en muchas ocasiones como burocrática y lenta, a mediados de la década de los 90 surgió un movimiento cuyo objetivo era promover una metodología que fuese mucho más ágil y menos restrictiva.

Tiempo después, en concreto en 2001, se celebró en Snowbird (Utah) una convención de informática y fue allí donde un grupo de personas adoptaron el nombre de «métodos ágiles» para denominar a este nuevo movimiento. De todas formas, es importante recordar que antes del 2000 ya fueron creados muchos métodos similares al ágil. Entre los más notables se encuentran, por ejemplo: Scrum (1986), Crystal Clear, programación extrema (en inglés eXtreme Programming o XP, 1996), desarrollo de software adaptativo, *feature driven development*, Método de desarrollo de sistemas dinámicos (en inglés, *Dynamic Systems Development Method* o DSDM, 1995).

Con el paso del tiempo, todas estas metodologías se fueron asentando y, hoy es el día en que muchas organizaciones hacen ya uso de algunas de ellas.

OTROS ÁMBITOS

Como hemos visto, las llamadas «metodologías ágiles» no son algo nuevo y se vienen usando desde hace tiempo, aunque principalmente en la **planificación** y en el **desarrollo** de software.



Dado que la informática abarca la planificación, desarrollo e implantación de un software, se puede decir que había/hay un «salto» entre la metodología que se usaba a la hora de desarrollar software y el procedimiento que se sigue a la hora de implantar las aplicaciones dentro de la

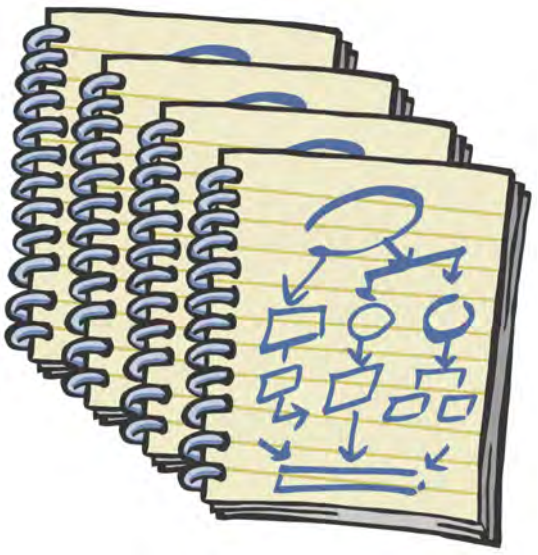
infraestructura o CPD de una organización. Y eso es un problema.

Para superar ese «salto», algunas iniciativas abogan por **extender el alcance de las metodologías ágiles** al ámbito de las infraestructuras y la administración de sistemas. Y es ahí donde surge el concepto DevOps.

[ver cuadro *«Infraestructuras ágiles»*]

EL ORIGEN DE DEVOPS

Históricamente, las metodologías ágiles permitían a una empresa lanzar (entregar) con mayor frecuencia el software que



desarrollaban para sus clientes. El problema que tenían estas empresas era que tenían que adecuar el ritmo de muchos de sus procesos internos para que todas las áreas implicadas estuviesen alineadas: gestión de versiones, lanzamiento de aplicaciones, herramientas de integración continua y la entrega continua.

«Las "metodologías ágiles" se vienen usando desde hace tiempo, aunque principalmente en la planificación y en el desarrollo de software»

Algunas empresas, por ejemplo, realizan más de diez despliegues diarios. A este tipo de sistemas se les conoce como «despliegues continuos» (*continuous deployment*) o «entregas continuas» (*continuous delivery*).

La idea de los **despliegues continuos** consiste en hacer integraciones de un proyecto lo más a menudo posible para así detectar los fallos cuanto antes.

La integración incluye la compilación y ejecución de las pruebas de todo un proyecto, y el proceso suele ser el siguiente: cada cierto tiempo (por ejemplo, cada pocas horas), se descargan las fuentes desde la aplicación que se usa para el control de versiones, por ejemplo Git[2], se compila, se ejecutan las pruebas necesarias

[2] **Git:** es un software diseñado por Linus Torvalds que facilita el control de versiones de las aplicaciones que desarrollamos, sobre todo cuando se trabaja con un gran número de archivos de código fuente. Mediante este software se puede llevar un registro de los cambios que se realizan en los archivos y permite coordinar el trabajo de varias personas.

Actualmente existen diferentes aplicaciones, como por ejemplo los siguientes:

- Basados en el Modelo Cliente Servidor:
  - Concurrent Versions System (CVS)
  - Subversion (svn)
  - AccuRev
  - Visual SourceSafe
- Basados en el Modelo distribuido:
  - Aegis
  - Bazaar
  - Git
  - BitKeeper

Para más información, podéis consultar el artículo *«GitHub: plataforma social para la liberación de código»*, en el boletín Aurrera nº 54 (diciembre de 2015).

INFRAESTRUCTURAS ÁGILES

Los ingenieros Yhens Wasna y Patrick Debois son considerados los «padres» del término DevOps ya que surgió durante la charla sobre *«Infraestructura Ágil y Operaciones»* que impartieron en la conferencia *«Agile 2008»* celebrada en agosto de ese año en Toronto (Canadá).

Uno de los retos que se plantearon en ese encuentro fue cómo se podía llevar la filosofía de la metodología «ágil» al mundo de la infraestructura y la administración de sistemas.

Y es a partir de ese momento cuando el término DevOps empezó a extenderse poco a poco.

y se generan los informes correspondientes.

En definitiva, esta nueva forma de trabajar es muy recomendable para aquellas empresas que tienen que realizar entregas muy frecuentes o cada poco tiempo.

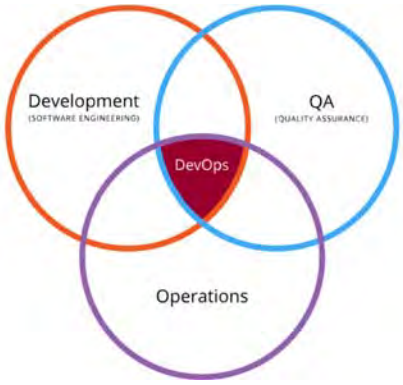
DevOps, por tanto, surge debido al éxito que tuvieron las metodologías ágiles a la hora de desarrollar software.

[3] **Gestión del cambio:** Todo cambio que quiera llevar a cabo una organización, implica un impacto mayor o menor en ella (en la Dirección, mandos intermedios, usuarios finales, estructura, tecnología...). Por ello, si se quiere completar con éxito ese cambio, es básico y fundamental el gestionar adecuada-mente ese proceso para, de esa forma, aprovechar las oportunidades, y superar las amenazas que se van a presentar durante el proceso.

Para más información, podéis consultar el artículo titulado *«Saber gestionar (bien) el cambio»*, publicado en el boletín Aurrera nº 30 (junio de 2008).

CAMBIO CULTURAL

Como suele ocurrir normalmente con cualquier novedad, para implantar con éxito la metodología DevOps en una entidad es necesario llevar a cabo una adecuada **gestión del cambio**[3], tanto desde un punto de vista cultural como organizativo.



[Imagen: Wikipedia]

El motivo es que esta nueva metodología se basa en impulsar la **colaboración**, la **comunicación** y la **integración de** áreas que, hasta ahora, han trabajado de forma aislada o estanca, como son el área de **Desarrollo** y la de **Sistemas** (algunas consultoras también incluyen los Equipos de **Seguridad** y de Ingeniería de **Calidad** como parte del nuevo modelo DevOps).

DevOps, por tanto, se basa en la integración entre desarrolladores/as software y administradores/as de sistemas.

En realidad, es un gran cambio que afecta tanto a los procesos como a las tecnologías y al equipo humano de cualquier organización o entidad. En definitiva, los cambios deben abordarse en toda la organización, y no sólo en el área responsable de las TICs, creando un modo de **trabajo multidisciplinar**, o incluso como algunas personas lo consideran... una nueva filosofía de trabajo.

Tanto es así que, para facilitar el trabajo de las personas implicadas, existen una serie de herramientas que pueden ser usadas en una o varias de las fases en que se divide el ciclo de vida de un producto software:

1. **Código fuente**: herramientas de desarrollo, revisión y administración de código fuente, fusión de código
2. **Construcción**: herramientas de integración y estado de compilación
3. **Prueba**: herramientas de prueba continuas
4. **Paquete**: repositorio de paquetes, distribución previa a la implementación de la aplicación
5. **Lanzamiento**: gestión de cambios, aprobaciones y automatización de versiones
6. **Configurar**: configuración y gestión de la infraestructura
7. **Control**: monitorización del rendimiento de las aplicaciones, experiencia del usuario final, etc.

Algunas de las aplicaciones que se pueden usar en algunas de esas fases son, entre otras, Solano CI, Bamboo, Pipeline, Apache Continuum, Hudson, Jenkins, GoCD, CruiseControl o Anthill (para proyectos

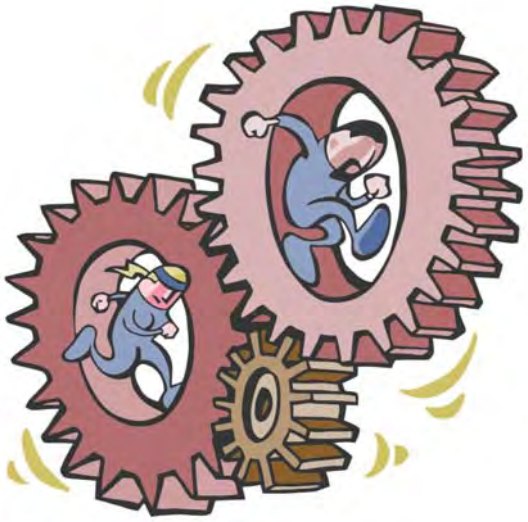
Java) o CruiseControl.Net, Team Foundation Build para .Net, que se encargan de controlar las ejecuciones, apoyadas en

«La idea de DevOps es extender el alcance de las metodologías ágiles al ámbito de las infraestructuras y la administración de sistemas»

otras herramientas como Ant o Maven (para proyectos Java), o Nant o MSBUILD (para .Net) que se encargan de realizar las compilaciones, ejecutar las pruebas y realizar los informes.

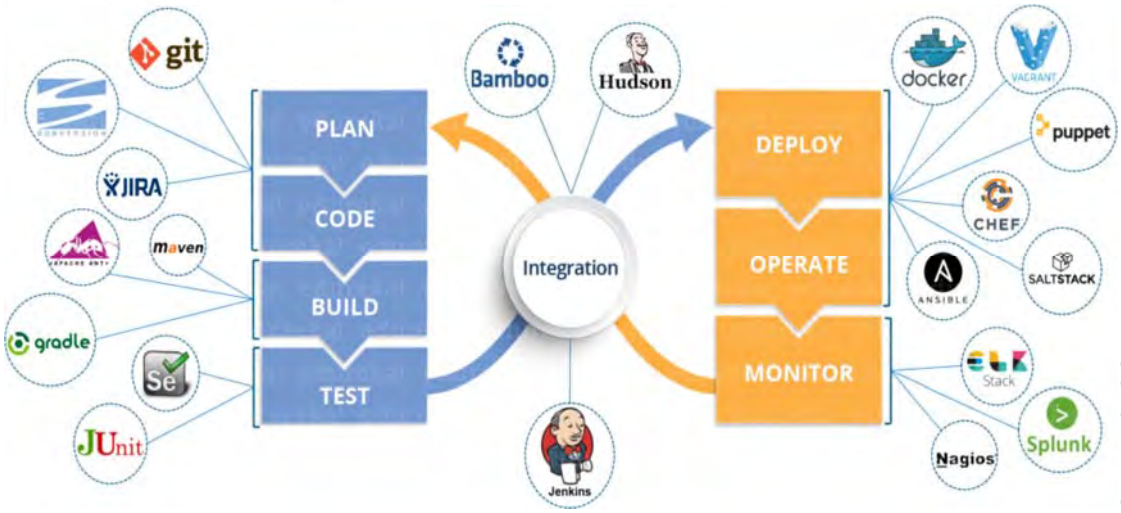
[ver esquema gráfico de las herramientas]

Todas estas herramientas y tecnologías, permiten automatizar el ciclo de vida de las aplicaciones[4]. Algunos de los procesos que hasta ahora solían ser manuales y lentos, como pueden ser, entre otros, actualizar el código, habilitar un nuevo entorno, etc., gracias a esta nueva metodología se pueden hacer de una forma mucho más rápida y continua. Además, también es más fácil cumplir las normas de seguridad, ya que estos aspectos están ya integrados en el propio proceso.



CONCLUSIÓN

Tal y como se ha comentado, el objetivo principal de esta nueva forma de trabajar denominada DevOps es responder con agilidad a las necesidades de la empresa, y ello se consigue mediante la realización continua de pruebas, la entrega continua y la supervisión continua. ❑



[Imagen: Edureka]

[4] **Ciclo de vida de las aplicaciones**: es el Proceso que se sigue a la hora de desarrollar una aplicación informática. Existen varios modelos a seguir, cada uno de los cuales tiene un enfoque diferente a la hora de organizar las diferentes actividades que tienen lugar durante ese proceso.

Existen varios tipos de modelos de desarrollo de software específicos, siendo los más conocidos los siguientes:

- ✓ En cascada
- ✓ En espiral
- ✓ Iterativo e incremental
- ✓ Ágil

Los viejos peligros de Internet: el phishing o la suplantación de identidades

Cada vez son más los peligros que nos acechan en Internet. Sin embargo, distintos estudios demuestran que la mayoría de ellos son viejos conocidos, y a pesar de ello siguen teniendo éxito. Veamos algunos ejemplos y cómo evitarlos.

Las fiestas navideñas en las que estamos inmersos son una época ideal para recibir mensajes de amigos y amigas (o empresas) que nos felicitan el año nuevo. Precisamente por ese motivo debemos tener especial cuidado con todos y cada uno de los mensajes que recibimos estos días, ya que detrás de ellos puede haber un serio peligro para nuestra «seguridad informática».

La razón es que algunos de esos mensajes podrían ser la puerta a través de la cual los y las hackers entran en nuestros sistemas para robarnos información personal o confidencial. Algunas de las técnicas más usadas para ello son, por ejemplo, la ingeniería social[5], los troyanos, el *phishing*, el *ransomware*[6]…

El método más habitual para obtener datos de una persona es mediante el envío de correos electrónicos que contienen troyanos, gusanos o virus que infectan nuestro ordenador y quedan a merced de los hackers o malhechores.

Asimismo, a medida que avanza la tecnología lo hace también el ingenio de las personas que se dedican a estafar a otras personas y se «cuelan» a través de los nuevos dispositivos móviles para obtener los datos de nuestras redes sociales o simplemente llamándonos al teléfono, simulando ser encuestadores o comerciales de una empresa que nos ofrecen cambios o mejoras en el servicio que tenemos contratados con ellos.

Las previsiones para 2019 apuntan a que los ataques serán más fuertes e inteligentes, tanto es así que ya ha surgido un nuevo nombre, el «*vaporworms*[7]», para definir un nuevo *malware*.

De todas formas, tengan un nombre u otro, el objetivo de todas esas técnicas es el mismo, llevar a cabo un ataque externo a una persona (o a una empresa) para obtener datos personales, confidenciales o privados y, posteriormente, haciéndose pasar por esa persona vaciar sus cuentas corrientes, comprar productos a su costa, etc.

En esta ocasión nos centraremos en el *phishing* o la suplantación de identidades.

EL PHISHING

Para empezar, diremos que el *phishing* es simplemente una modalidad de **estafa** donde una persona (a través de un e-mail, por ejemplo) se hace pasar por otra persona u otra empresa con el objeto de obtener de un usuario/a ciertos datos: su número de tarjeta de crédito, su contraseña...

Este tipo de «robo de identidad» basa su éxito en la facilidad con que muchas personas confiadas revelan información personal a los *phishers* o estafadores/as sin darse cuenta.

El funcionamiento del ataque es muy simple:

[5] **Ingeniería social:** la Ingeniería Social (del inglés *Social Engineering*) comprende todas aquellas tretas, engaños y técnicas utilizadas por un hacker para sacar información (una contraseña, por ejemplo) a una persona sin que ésta se dé cuenta de que está revelando «información sensible» o bien conseguir que ese usuario/a realice una acción concreta (p.ej. abrir un archivo que contenga un virus).

[6] **Ransomware:** término que resulta de la unión de dos palabras inglesas: *ransom* (rescate) y *ware* de soft*ware*. Consiste en un tipo de programa malicioso (*malware*) que restringe el acceso a nuestro ordenador ya que encripta nuestra información. Para poderla recuperar tendremos que pagar un rescate al hacker.

[7] **Vaporworms:** una nueva especie de *malware* sin archivos y con propiedades similares a las de un gusano, que le permiten autopropagarse a través de sistemas vulnerables, autoeliminarse de Internet y lanzar ataques de ransomware contra empresas.

El estafador o estafadora se hace pasar por una empresa e intenta hacer creer al destinatario/a que los datos solicitados se los pide la página web oficial, cuando en realidad no es así. Lo más curioso de este delito es que no es un ataque que requiera de herramientas y/o conocimientos muy sofisticados. Es más, las técnicas que se utilizan no son nuevas y son conocidas desde hace años.

«La SEGURIDAD de los Sistemas de Información no depende de una única persona, y todos/as debemos aportar nuestro granito de arena.»

El atacante puede usar varios canales para llegar al usuario/a final, es decir, su víctima:

- ✓ **Correo electrónico**: es el método más habitual. En este caso, se envía un e-mail a muchas personas simulando ser una entidad oficial para obtener datos de algunas de esas personas. Los datos son solicitados alegando motivos de seguridad, mantenimiento del ordenador, mejorar el servicio, responder a una encuesta o cualquier otra excusa, para que la persona elegida facilite sus datos secretos. El correo puede contener formularios, enlaces falsos, logotipos oficiales, etc., todo para que visualmente el mensaje parezca oficial y no levante sospechas. La idea final es que el usuario/a final facilite su información y (sin saberlo) lo envíe directamente al estafador/a, quien la usará más tarde de forma fraudulenta.
- ✓ **Página web**: en este caso se simula visualmente la página web de una entidad real, normalmente un banco. El objetivo es que el usuario teclee sus datos privados en un formulario que hay en esa web falsa.
- ✓ **Llamada telefónica**: el usuario/a recibe una llamada telefónica en la que el estafador/a suplanta a una entidad para que ese usuario/a le facilite también datos privados. Un ejemplo típico es el que se produce en la época de la Declaración de la Renta, donde los ciberdelincuentes llaman a los contribuyentes para pedirles datos de su cuenta corriente haciéndose pasar por personal de Hacienda, amenazándoles que si no lo hacen serán sancionados.

Normalmente, los servicios más suplantados son los relacionados con el dinero (Banca on-line, Servicios de subastas en línea y Tarjetas de crédito). La razón es que un atacante con la clave de un usuario podría manejar ese dinero sin ningún problema y transferirlo a otra cuenta bancaria.

Otro ataque similar basado también en la suplantación de identidades puede ser, por ejemplo, cuando un usuario/a de una organización recibe una llamada de «su» Administrador de Sistemas o del Centro de Atención a personas Usuarias [CAU] (y mediante este engaño) pedirles directamente sus contraseñas.

Recientemente, ha saltado a los medios de comunicación el fraude sobre un supuesto servicio técnico de Microsoft, que ya fue utilizado hace algún tiempo, aunque vuelve a estar en auge otra vez. En este caso, los delincuentes se ponen en contacto con ciudadanos particulares (e incluso con personas que trabajan en el sector público).

El funcionamiento es el siguiente: normalmente una persona que habla un mal inglés se pone en contacto con nosotros mediante una llamada telefónica. El hacker nos comunica que desde nuestro ordenador, que supuestamente está infectado por un virus, se está atacando a organismos del Gobierno de los Estados Unidos, y que nos van a ayudar a «limpiarlo». Para ello, nos aconseja descargar y ejecutar un software de control remoto (normalmente el programa Teamviewer), nos solicita nuestra identificación de sesión y nos piden

ARTÍCULOS

A continuación, os incluimos algunos de los artículos publicados en el boletín Aurrera relacionados con los ciberdelitos y la seguridad informática:

- ➢ *«Seguridad: virus»* (Aurrera nº 3, marzo de 2001)
- ➢ *«Ingeniería Social»* (Aurrera nº 13, marzo de 2004)
- ➢ *«EJIE: Los virus y ataques informáticos»* (Aurrera nº 14, junio de 2004)
- ➢ *«Ransomware: amenaza en auge»* (Aurrera nº 55, marzo de 2016)
- ➢ *«Robo de datos en internet»* (Aurrera nº 61, septiembre de 2017)
- ➢ *«Centro Vasco de Ciberseguridad (BCSC)»* (Aurrera nº 63, marzo de 2018)

autorización para tomar el control de nuestro propio ordenador. A partir de ahí bajan un software que cifra la información de nuestro ordenador, y, en este caso, nos solicitan un «rescate» para poder recuperarla. El «rescate» se pagará en «bitcoins» para evitar ser rastreados. Y suele ocurrir que, aunque se pague, el ordenador continúe con la información cifrada, con lo que seguiremos a su merced.

CONTRAMEDIDAS

La mejor manera de evitar este tipo de peligros (o reducir lo más posible su impacto) es estar bien informados/as. Para ello, el Gobierno Vasco, dentro el **plan de formación** que coordina e impulsa el Comité de Seguridad y Privacidad, denominado **GureSeK**[8], ha llevado a cabo a lo largo de los últimos meses varios simulacros usando mensajes falsos.

Os presentamos a continuación un breve resumen de los resultados obtenidos:

A lo largo de 2017, el Gobierno Vasco envió a todo su personal (5.960 personas en total) tres correos electrónicos falsos simulando un ataque de *phishing*.

En el primero de ellos, por ejemplo, se solicitaba al usuario o usuario final que pinchase un enlace (que aparecía en el propio mensaje) para que cambiase su contraseña en una página web externa.

«La mejor manera de evitar este tipo de peligros es estar bien informados/as»

En el segundo caso, el correo electrónico simulaba ser un aviso de la empresa Correos, y que debíamos acceder a una página facilitando nuestros datos para poder recoger un paquete.

Y, en el tercer y último de ese año, se envió un correo en nombre de la multinacional Amazon donde se ofrecía al usuario/a una tarjeta regalo a cambio de que facilitase sus datos personales.

Este mismo año, en 2018, también se ha llevado a cabo una nueva campaña de emails falsos y los resultados de la misma han sido los siguientes:

La última campaña se desarrolló entre el 5 y el 9 de noviembre de 2018. En este caso, se usó como señuelo un mensaje de correo electrónico **de una supuesta alerta remitida desde una falsa «Microsoft corps. keys».**

[8] **GureSeK:** se denomina GureSeK (del euskera, «*Gure Segurtasun Kudeaketa*») al proceso o Sistema de Gestión de la Seguridad de la Información (SGSI) encargado de gestionar la seguridad de los servicios electrónicos prestados a la ciudadanía y a las empresas por parte de la Administración General de la Comunidad Autónoma de Euskadi y sus Organismos Autónomos (Departamentos y Organismos Autónomos).

El número de ordenadores del Gobierno Vasco en el que se recibió este mensaje fue de 5.435 en total y el número de personas que hizo click, es decir, que pulsó el enlace falso que aparecía en el mensaje, fue de 1.620 (un 29,81%).

El CAU recibió un total de 133 incidencias o llamadas avisando de este mensaje sospechoso (2,45%), de las cuales la mayoría de ellas tuvieron lugar el martes 6 (debido a ello, el CAU habilitó una grabación para atender a los usuarios/as que llamaban y no saturar el resto del servicio).

CONCLUSIÓN

Aunque el grado de concienciación es cada vez mayor, y los resultados obtenidos están por debajo de la media con respecto a otras organizaciones similares, una de las conclusiones obtenidas es que sigue habiendo un numero alto de personas que «caen» en la trampa y pinchan en estos enlaces falsos que se les envía en el correo electrónico.

Por ello, el objetivo final de todas estas iniciativas o simulacros (y las que se puedan llevar a cabo en el futuro) es **crear conciencia sobre la seguridad** en todo el personal que forma parte de nuestra organización (incluso, entre aquellas personas que no tienen acceso directo a un ordenador o a algún otro dispositivo electrónico), ya que la SEGURIDAD de los Sistemas de Información no depende de una única persona, y todos/as debemos aportar nuestro granito de arena. ❑

Recomendaciones

Aquí os dejamos algunos consejos básicos que debemos tener en cuenta para estar informados de estos peligros o los pasos a seguir cuando detectemos una situación sospechosa:

- ✓ Asistir a charlas o cursos de formación sobre seguridad.[9]
- ✓ Nunca abrir archivos adjuntos (incluso si el remitente es conocido/a) si no los hemos solicitado previamente, especialmente si es un archivo .exe, .doc, .wls,.vbs o .xls.
- ✓ Manejar con precaución las URLs (direcciones webs) adjuntas en los correos. El «*phishing*» utiliza URLs falsas para tentar a los usuarios a visitar ciertas páginas de Internet. Estas páginas usurpan sitios webs legítimos para solicitar información sensible como contraseñas o números de cuentas.
- ✓ Nunca informar por teléfono de las características técnicas de la red, sus localizaciones físicas o personas a cargo de la misma y, menos aún, información sobre Usuarios y Claves de acceso a ordenadores. (es aconsejable comprobar previamente la veracidad de la fuente que solicita dicha información).

- ✓ Nunca tirar documentación técnica (o que contenga información personal) a la basura, sino destruirla. Suele ser habitual tirar a la papelera gran cantidad de datos confidenciales sin darnos cuenta (o dejar un papel debajo del teclado o en el cajón con nuestra *password*, etc.)
- ✓ Informar sobre conductas sospechosas (por ejemplo, si vemos personas no autorizadas que utilizan un ordenador al que no deberían tener acceso, etc.)
- ✓ Si somos contactados por alguien que busca acceso no autorizado a cierta información, debemos informar inmediatamente al CAU (Centro de Atención a personas Usuarias) o a la persona que ocupa el puesto de Responsable de Seguridad dentro de nuestro Departamento y seguir sus indicaciones para intentar rastrear el origen de la llamada o del correo electrónico recibido.

[9] **Formación sobre seguridad**: dentro del catálogo de cursos que ofrece el IVAP, tenemos el titulado «*Seguridad de la información en el ámbito de la Administración electrónica*» (en formato online y con una duración de 10 horas), siendo su temario el siguiente:

- Bloque I: Gestión de la seguridad
  1. Conceptos de seguridad de la información
  2. Esquema Nacional de Seguridad (ENS)
  3. Derechos de las personas en sus relaciones con las administraciones públicas
  4. Firma electrónica
  5. Copias de seguridad
- Bloque II: Casos prácticos
- Bloque III: El puesto de trabajo corporativo
- Bloque IV: Marco normativo

Para más información consultar la web:

www.ivap.eus

ALBOAN:

Parque móvil del Gobierno Vasco. Un paso más en la digitalización del servicio

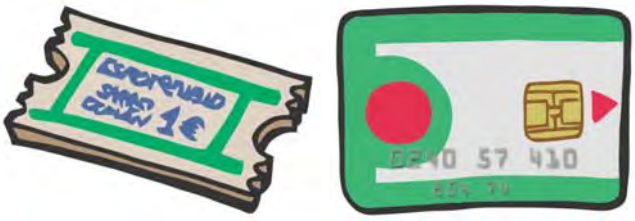
«El nuevo módulo hace uso de distintas soluciones de la Plataforma Tecnológica PLATEA del Gobierno Vasco»

Según se recoge en el Decreto 71/2017, de 11 de abril, por el que se establece la estructura orgánica y funcional del Departamento de Gobernanza Pública y Autogobierno, a la **Dirección de Recursos Generales** le corresponderán, entre otras, las competencias relativas a la *«ordenación, gestión y administración de los servicios y vehículos del Parque Móvil de la Administración»*.

DIGITALIZACIÓN

El Servicio de Parque Móvil gestiona actualmente alrededor de **600 vehículos** y su principal función es facilitar estos vehículos a las personas del Gobierno Vasco que por motivos laborales así lo requieran. En esos casos, se deberá solicitar a través de la **aplicación M05J**, la cual está accesible en Jakina.

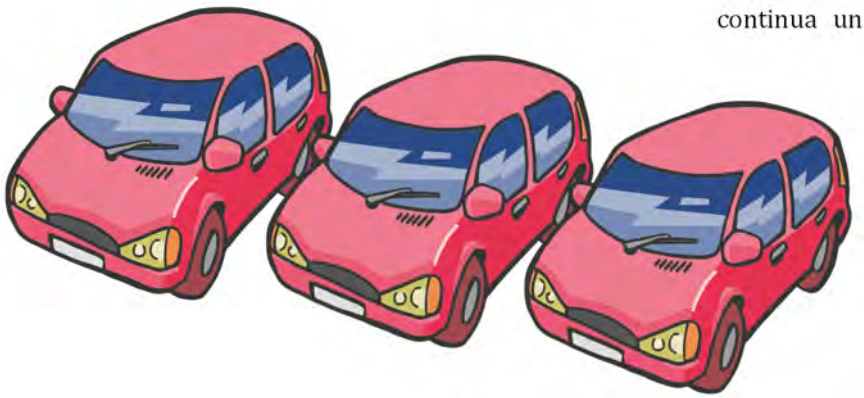
Mensualmente, las personas que tienen asignado un coche de forma continua remiten al Servicio de Parque Móvil (en formato papel) los **tickets y/o recibos originales** de los gastos en que han incurrido y que deben ser justificados. Posteriormente, la persona encargada del Servicio de Parque Móvil introduce todos y cada uno de los conceptos que aparecen en esos tickets (fecha, importe, etc.) en la aplicación para ser validados.



Este procedimiento ha provocado en ocasiones algún problema, por ejemplo, cuando no se aportan todos los tickets o cuando los tickets no llegan correctamente.

Con objeto de mejorar el servicio y su gestión, la Dirección de Recursos Generales recientemente ha desarrollado una importante mejora en la **aplicación M05J**, incluyendo una nueva utilidad o módulo, llamado «Justificación de gastos», cuyo principal objetivo es eliminar ese intercambio de papel (tickets y resguardos de pago) que actualmente existe entre los Departamentos y el Servicio de Parque Móvil.

Gracias a esta mejora las personas que tienen asignado en estos momentos de forma continua un coche (alrededor de 300) ya pueden introducir directamente en la aplicación los datos de sus propios gastos: la fecha del ticket, concepto a imputar, importe del gasto, etc., y **sin tener que intercambiar ni un sólo documento en soporte papel**, ya que los tickets o resguardos se adjuntarán al



expediente quedando almacenados en la propia aplicación. Además, permitirá a cada usuario/a consultar el histórico de tickets introducidos.

Gracias a este nuevo módulo se consiguen varias mejoras: se evitan errores a la hora de introducir los datos, se consigue reducir totalmente el intercambio de papel entre los Departamentos y la Dirección de Recursos Generales, se evitan perdidas de tickets, etc.

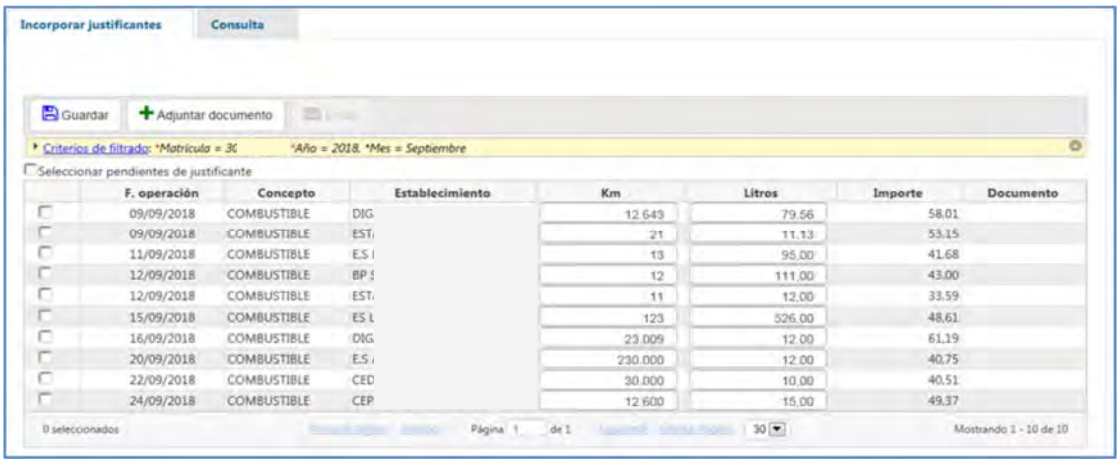
Esta nueva funcionalidad se irá extendiendo para que pueda ser usada por todo el personal del Gobierno Vasco.

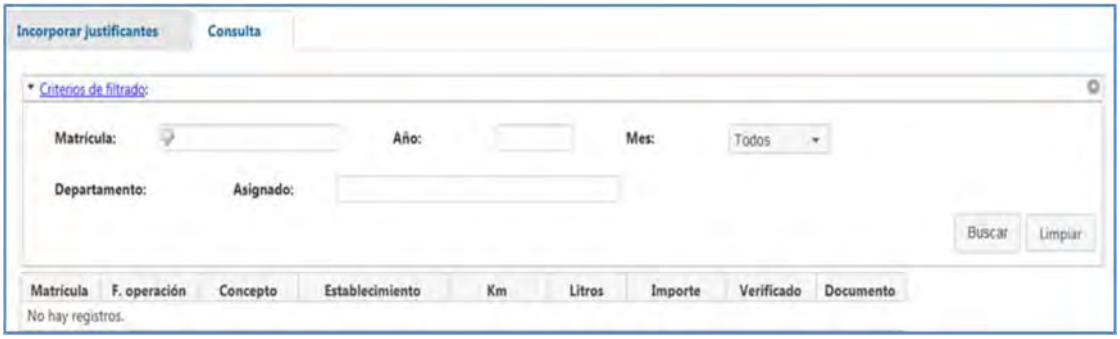
ASPECTOS TÉCNICOS

Desde el punto de vista más técnico indicar que el nuevo módulo ha sido desarrollado por el personal de la sociedad pública EJIE usando J2EE como plataforma de desarrollo y basándose en la última versión del Framework UDA. Está soportada en Weblogic 11g (como Servidor de aplicaciones) y utiliza Oracle 12c como Servidor de Base de Datos. La gestión de la seguridad, es decir, la identificación de usuarios/as, está integrada con XLNets para su uso en la intranet JASO del Gobierno Vasco. Además, los documentos que adjuntan los Departamentos y Organismos Autónomos se integran en el Sistema Integral de Gestión Documental del Gobierno Vasco, dokusi.

De todas formas, las mejoras de la aplicación M05J de Parque Móvil no acaban aquí, ya que a lo largo del próximo año se tiene previsto ir desarrollando nuevas funcionalidades que se están planificando y que os iremos presentando. ❑

«El objetivo del proyecto es eliminar el intercambio de papeles entre los Departamentos y el Servicio de Parque Móvil»





Normativa:

Decreto 300/1999, de 27 de julio, por el que se regula el Parque Móvil de la Administración General

ALBOAN

¡¡Contraportada!!

Nº 66

diciembre 2018

AL CIERRE

LibreCon2018

El 21 y 22 de noviembre pasados se celebró en el Palacio Euskalduna de **Bilbao** una nueva edición de LibreCon, el mayor encuentro empresarial sobre Software Libre y Código Abierto.

A lo largo de esos dos días tuvimos la oportunidad de ver las presentaciones de algunas de las empresas más innovadoras en ofrecer soluciones *open source*.

Tanto el Gobierno Vasco como la Sociedad Informática EJIE tomaron parte en dicho evento con una **mesa redonda** titulada *«Liberar o reutilizar ¿Dónde debe poner el foco la Administración Pública?»*, moderada por la Viceconsejera de Administración y Servicios Generales Nerea Lopez-Uribarri Goicolea, donde se explicó el éxito de la Plataforma de Contratación Electrónica de Euskadi y se reflexionó sobre cuáles deberían ser los próximos pasos que debería dar el Gobierno Vasco para cumplir la normativa vigente en materia de reutilización de software.

Así mismo EJIE (de la mano de Oscar Guadilla) impartió una **ponencia** titulada *«Blockchain: nuevo modelo de colaboración en la Administración Pública»*, donde se expusieron algunas de las iniciativas que se están llevando a cabo y posibles colaboraciones con otras Administraciones.

+info: http://www.librecon.io

PROTAGONISTAS

Hedy Lamarr, inventora

La actriz, inventora e ingeniera de telecomunicaciones Hedy Lamarr (1914-2000) nació un 9 de noviembre. Junto al compositor George Antheil, inventó una primera versión del espectro ensanchado —técnica de modulación empleada en telecomunicaciones—. El **Día Internacional del Inventor** se celebra precisamente cada 9 de noviembre en su honor.

Su primer marido fue uno de los hombres más influyentes de Europa y, antes de la Segunda Guerra Mundial, se dedicó a surtir el arsenal de Hitler y Mussolini. Por ello, fue considerado como ario honorario pese a ser de origen judío.

Como Hedy no podía hacer nada sin la autorización de su marido, y hastiada del vacío insoportable en el que se había convertido su vida, retomó la carrera de ingeniería. En las reuniones de trabajo a las que asistía, aprovechó para aprender y recopilar información sobre las características de la última tecnología armamentística nazi.

Tras conseguir huir a EE.UU., Hedy ofreció su preparación como ingeniera al recientemente creado *National Inventors Council*. Junto con su amigo Antheil registraron en junio de 1941 la patente del *Secret Communication System*.

La patente interesó a los militares, pero suscitó diversas opiniones. La marina de EE.UU. Indicó que el sistema era excesivamente vulnerable y engorroso y archivó el proyecto. Lamarr y Antheil se olvidaron del tema y volvieron a la cinematografía. No fue hasta 1957, que ingenieros de la empresa estadounidense Silvania Electronics Systems Division desarrollaron el sistema patentado por Hedy y George, que fue adoptado por el Gobierno para las transmisiones militares tres años después de caducar la patente

[Extracto del artículo publicado en https://mujeresconciencia.com/2015/11/30/hedy-lamarr-la-inventora/