gmv® INNOVATING SOLUTIONS NEWS

Nº65

AGOSTO 2017

www.gmv.es

CIBERSEGURIDAD

EVOLUCIÓN, TENDENCIAS Y NUEVAS AMENAZAS

ENTREVISTA

ALBERTO HERNÁNDEZ

Director General del Instituto Nacional de Ciberseguridad de España (INCIBE)

TALENTO Antonio Lozano Lima. *"Las becas de GMV están llenas de oportunidades, tanto para la empresa como para los estudiantes"*

rbr EVENTS

ATM & Cyber Security 2017

(formerly 'ATM Security')

#ATMsec

London 10th-11th October 2017

VEN Y VISÍTANOS

ATM & Cyber Security 2017

Londres (Reino Unido), 10-11 octubre

ATM & Cyber Security 2017 es la conferencia líder del mundo centrada en la seguridad ATM física y lógica. El evento atrae a más de 340 asistentes, representando a más de 140 organizaciones de más de 40 países en todo el mundo.

GMV junto con el departamento de investigación de Trend Micro FTR (*Forward-looking Threat Research*), realiza una ponencia bajo el título "La naturaleza específica del malware ATM". Una conferencia para ilustrar cómo el malware ATM difiere sustancialmente del malware clásico orientado a PC y cómo la protección debe adaptarse en consecuencia. David Sancho, Investigador Anti-Malware en Trend Micro, y Juan Jesús León, Director de Productos y Nuevos desarrollos en GMV Secure e-Solutions, presentan nueva información (no publicada antes).

Más información:
https://www.rbrlondon.com/events/atmsec

gmv® INNOVATING SOLUTIONS

CARTA DE LA PRESIDENTE

Internet es una red universal, usada a diario por miles de millones de personas. Los usuarios de internet, con acceso a un punto de conexión y los conocimientos básicos necesarios para su uso, ya abarcan algo más del 50% de la población mundial. Usamos internet para comunicarnos con colegas, amigos y familiares, para ver vídeos y películas, para hacer transacciones bancarias, para comprar artículos de todo tipo, para leer libros, para ver los horarios del autobús o pedir un taxi, para obtener información. Google ejecuta 2.5 millones de búsquedas por minuto, lo que equivale a una media de una búsqueda diaria por cada usuario de internet.

Más allá de las personas, cada día hay más dispositivos conectados a internet. Hace una década, internet estaba compuesto básicamente por computadoras. Después llegaron los smartphones, y ahora se están conectando todo tipo de aparatos, incluyendo sensores industriales, aparatos domésticos y dispositivos personales. Es el internet de las cosas, o mejor expresado, el internet de todo.

Internet y los dispositivos conectados están revolucionando nuestras vidas, posibilitando con un click gestiones que sin ellos serían mucho más complicadas, incómodas o incluso imposibles. A cambio estamos entregando cantidades ingentes de información nuestra y sobre nosotros. Mientras publicar un mensaje o una foto en las redes sociales es una decisión, acertada o no, pero activa, no tenemos ese mismo control sobre la información que manda nuestro smartphone, nuestro televisor o el último gadget que nos hemos comprado, de la que a menudo no conocemos ni el contenido ni el receptor. Las tecnologías de Big Data e Inteligencia Artificial van a impulsar la capacidad de evaluar todos esos datos. Debemos ser conscientes de ello y retomar el control aplicando mecanismos de Ciberseguridad.

Mónica Martínez

Nº 65
AGOSTO

CONTENIDOS

Edita
GMV

Dirección-Coordinación
Marta Jimeno, Marta del Pozo

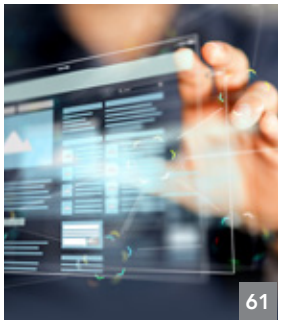
Responsables de área
Antonio Hernández, Miguel Ángel Molina, José Prieto, Isabel Tovar

Redacción
Neusa de Almeida, Amaya Atencia, Julián Barrios, Mariano Benito, Maole Cerezo, Iker Estébanez, Pedro Fernandes, Raquel Fernández, Teresa Ferreira, Fernando Gandía, Ángeles García, Celestino Gómez Javier Gómez, Bruno Gonçalves, David González, Sara Gutiérrez, Raúl Herbosa, Antonio Hernández, Fernando Labarga, Pedro Lopes Vieira, Fátima López, Antonio Lozano, Belén Martín, Kamil Martin, David Merino, Daniel Montero, Héctor Naranjo, José Neves, Begoña Ochoa, Tatiana Pagola, Andrea Pellacani, Eric Polvorosa, Marta del Pozo, José Prieto, Pablo Rivas, Miguel Romay, Javier Sanz, Ian Sephton, Daniel Silveira, Juan Tejo, Javier Zubieta.

Arte, diseño y maquetación
Francisco Huertas, Paloma Casero

MÁS INFORMACIÓN
marketing@gmv.com
+34 91 807 21 00

6


61


34


53


48


45


20


13

El pasado 13 de mayo, las televisiones abrían por primera vez sus informativos con una noticia de Ciberseguridad (el ataque WannaCry), en lugar de con la habitual actualidad política, económica, deportiva o de sucesos. No fue una sorpresa para GMV, que de hecho intervino en los informativos aportando respuestas para las preguntas básicas: ¿Qué pasó? ¿Por qué pasó? ¿Cómo resolver el problema y evitar que se repita?

La transformación digital en la que están embarcadas las organizaciones y que las expone a este tipo de ataques no es una moda, es una tendencia de mercado. GMV ya nació como una empresa digital, por lo que es consciente tanto de las ventajas que conlleva esta transformación digital como de los problemas de Ciberseguridad que le son inherentes, de los que WannaCry es solo un ejemplo. Por ello, GMV lleva trabajando desde el siglo pasado en su propia Ciberseguridad y en la de sus clientes, y tiene la capacidad, medios y conocimiento necesarios para asegurar y proporcionar los niveles de protección adecuados para cada caso. Protección que necesita la propia organización, sus procesos productivos y/o de prestación de servicios y también la creciente información que maneja o genera en su actividad.

Para nada es una tarea simple. GMV misma puede recibir ataques generales, pero como empresa innovadora en mercados de alta tecnología, se sabe en el punto de mira de atacantes a la Propiedad Intelectual, metodologías de trabajo o software de la compañía. Atacantes que están perfectamente organizados, que cuentan con los medios más eficaces y la máxima motivación para ejecutar estos ataques y que se ocultan en cualquier país del mundo, detrás de cualquier equipo conectado, lo que dificulta enormemente la detección y detención de los ataques antes de que ocurran. Y dificulta más aun la toma de acciones de respuesta.

Aun así, GMV lo consigue. Para ello, cuenta con la dedicación continua de personal fuertemente especializado en Ciberseguridad, dotado de un conocimiento tecnológico excelente y continuamente actualizado, con presencia continua en los foros y redes donde se discuten y se trabajan las tecnologías y vectores de ataque aparecidos en las últimas horas. Cuenta también con la concienciación y compromiso de toda la compañía de no ser el eslabón débil, el "garbanzo negro" de la Ciberseguridad que origine un incidente. Y con un fuerte componente de innovación, creación y aprendizaje de Ciberseguridad. Todo ello coordinado mediante metodologías, certificaciones y sistemas de gestión propios, lo que garantiza que cada vez que ocurra un incidente, encontrará a GMV prevenido, preparado, actualizado y trabajando en ello.

Por ello, GMV es una garantía de Ciberseguridad. Estamos preparados para lo que pueda venir, tanto a nosotros, como a nuestros clientes.

Mariano J. Benito
CISO
GMV SECURE e-SOLUTIONS

CIBERSEGURIDAD
Evolución, tendencias y nuevas amenazas

EN UN ESCENARIO REAL DEBEMOS ASUMIR QUE VAMOS A SER ATACADOS. POR LO TANTO, PARECE RAZONABLE INCREMENTAR LOS ESFUERZOS PARA MINIMIZAR EL IMPACTO DE LOS ATAQUES. CUANTO MÁS SOFISTICADO SEA EL ATAQUE, MÁS DIFÍCIL SERÁ DE DETECTAR Y CUANTO MÁS TARDEMOS EN DETECTAR, TENDREMOS MAYOR EXPOSICIÓN AL RIESGO

LA CIBERSEGURIDAD ESTÁ EN LA CALLE

Después de la campaña WannaCry de mayo de 2017 hemos notado una "popularización" de la Ciberseguridad, que ha servido para que las palabras "ciberataque", "ransomware" o "parche" aparecieran en las conversaciones entre particulares, aunque sólo fuera por unos días.

Esta situación, muchas veces criticada desde el lado profesional, trae consigo efectos positivos y negativos. Al menos eleva el nivel de sensibilización, algo bastante demandado durante muchos años, pero no debemos de caer en el sensacionalismo, sino simplemente aprovechar el momento para poder elevar la Ciberseguridad al lugar donde le corresponde: servir y proteger, ya sea a las organizaciones, a los países o a los particulares.

La labor de evangelización sigue siendo imprescindible. No sólo se trata de ser excelente en la actividad que se realiza: también hay que demostrarlo y difundirlo. En ese sentido, el impulso de difusión de conocimiento que desde GMV se está realizando es francamente notable, destacando en redes sociales, en la comunidad académica o en medios de comunicación tanto especializados como generalistas, donde ahora mismo nos consideramos creadores de opinión.

ATAQUES SOFISTICADOS, QUE REQUIEREN RESPUESTAS SOFISTICADAS

Las amenazas a las que nos enfrentamos son bien conocidas, al igual que las motivaciones de quienes intentan materializarlas. Tampoco es novedosa la sofisticación con la que se orquestan y perpetran ciertos ciberataques actuales pero sí llama la atención que, en general, la respuesta desde el "lado del bien" debería mejorar. No nos referimos a responder atacando, más bien a la contención de los daños y a la vuelta a la normalidad, es decir, a la resiliencia.

En un escenario real debemos asumir que vamos a ser atacados, ya sea de forma sofisticada o burda. Por lo tanto, parece razonable incrementar los esfuerzos para minimizar el impacto de los ataques. Es cierto que cuanto más sofisticado sea el ataque, más difícil será de detectar y cuanto más tardemos en detectar, tendremos mayor exposición al riesgo. Esto se puede mitigar utilizando Inteligencia de Ciberseguridad, algo que en GMV sabemos hacer.

La Inteligencia requiere analizar una cantidad brutal de información, para lo que utilizamos las tecnologías de análisis predictivo depuradas por nosotros dependiendo del contexto en el que se utilicen. Por ejemplo, en la lucha contra el fraude bancario tenemos amplia experiencia en definir y refinar algoritmos de análisis de comportamientos que se salen "de lo

normal" para poder detectar intentos de fraude provocados por software malicioso tipo Dridex. Otro ejemplo es la lucha contra el fraude cuyo objetivo es el propio cajero automático y su dinero, en donde llevamos más de una década empleando nuestra tecnología ***checker ATM Security***, alcanzando el liderazgo a nivel mundial.

GESTIÓN DE LAS VULNERABILIDADES, PASO DE GIGANTE

Paradójicamente, el nivel de sofisticación de los ataques contrasta muchas veces con la simplicidad de ciertos métodos que se repiten constantemente. En la práctica totalidad de los ciberataques existe un momento en el que se cuelan por un agujero, lo que entendemos como aprovechamiento de una vulnerabilidad no resuelta. Resulta curioso, a la vez que frustrante, constatar que muchos de los ciberataques más exitosos aprovechan vulnerabilidades conocidas desde hace años y fáciles de resolver empleando una dotación mínima de recursos.

Cuando se habla de riesgo, nos referimos a la combinación de la probabilidad de que se materialice una amenaza junto con el impacto que provocaría. La gestión de las vulnerabilidades incide principalmente en la probabilidad, disminuyéndola de forma significativa y, por lo tanto, disminuyendo el riesgo. Si esto lo unimos al hecho de que raro es el ciberataque que no hace uso de una vulnerabilidad no resuelta, podemos concluir que una gestión de vulnerabilidades profesional y bien articulada puede suponer un paso de gigante en la carrera que libramos contra aquellos que nos atacan.

La gestión de las vulnerabilidades es una práctica bien conocida por los departamentos de Ciberseguridad de las organizaciones, se lleva haciendo muchos años y cada vez se refina más y más. Se ha estandarizado un proceso de tratamiento con muchísimo sentido común, que empieza por el descubrimiento, continua por la depuración y constatación, le sigue la determinación de las acciones correctoras y termina con la información a los afectados, todo ello de forma cíclica para su seguimiento.

Una gestión de vulnerabilidades profesional y bien articulada puede suponer un paso de gigante en la carrera que libramos contra aquellos que nos atacan

En GMV hemos optimizado al máximo este proceso de gestión a través de ***gestvul***, un servicio creado en la casa para mantener a raya las vulnerabilidades en dos contextos especialmente complejos. El primero, en aquellos escenarios donde el número de activos es muy elevado y una gestión "al uso" puede naufragar estrepitosamente debido a un problema de escalabilidad. El segundo, en aquellos escenarios donde el número de partes interesadas o afectadas es también muy elevado, resultando crítica la información que estas partes deben disponer en plazo y en forma.

A MÍ... ¿QUIÉN ME VA A ATACAR?

Lamentablemente es bastante frecuente creer que no vamos a ser una víctima de un ciberataque. Frases del estilo "a mí... ¿quién me va a atacar?" las escuchamos demasiadas veces. Son especialmente frecuentes en el sector industrial, donde la concienciación sobre los riesgos ciber es mejorable y las medidas efectivas de ciberprotección de estas compañías no están tan maduras como sería deseable, sobre todo en las instalaciones y redes industriales.

Toda la experiencia de la práctica de Ciberseguridad alcanzada en los últimos años puede ser de aplicación en los entornos industriales, con su obligada particularización. Incluso podemos aprovechar el impulso que está dando el negocio alrededor de las iniciativas Industria 4.0 o Transformación Digital, para poder incorporar la Ciberseguridad desde origen y no a posteriori, cuando ya sería demasiado tarde. Debe actuar como un facilitador y como ya se ha mencionado anteriormente, adquiere especial protagonismo en tres actividades clave: prevención, estar lo más preparados posible ante las amenazas existentes; contención, poder minimizar al máximo el impacto de un ataque; y recuperación, poder restablecer la normalidad lo antes posible después de una contingencia sufrida.

GMV ha adquirido una gran experiencia en Ciberseguridad para entornos industriales con especial relevancia en el sector energético y en el sector aeroespacial. Abarcamos todo el ciclo de vida de los niveles de seguridad definido en el ISA/IEC 62443, analizando la situación actual a través de los "cyber-assessments", implementando medidas de protección en sistemas y redes IT y OT, operando y monitorizando los controles definidos y, todo ello, a través de un sistema de gestión y un marco de gobierno de toda la actividad de Ciberseguridad Industrial.

PROFESIONALES ALTAMENTE DEMANDADOS

Se ha convertido en una constante en el 2017: faltan expertos en Ciberseguridad a nivel mundial. Los analistas se aventuran y lo cuantifican entre 1,5 y 2 millones de puestos sin cubrir para el 2019.

La dificultad a la hora de encontrar personal altamente cualificado provoca que las organizaciones sean extremadamente exigentes a la hora de contratar un servicio de Ciberseguridad a un proveedor externo como GMV. La exigencia se dirige a la especialización (no valen los servicios genéricos, deben ser específicos) y a la adaptación a la organización (no valen los servicios estandarizados o rígidos, deben ser totalmente flexibles y adaptables a la cultura y el día a día del cliente). O lo que es lo mismo: aptitud + actitud.

En realidad estos requisitos siempre han estado ahí. Lo novedoso es el nivel de sofisticación actual que llega hasta el punto de que muchos servicios se prestan totalmente a medida del cliente. Como consecuencia, adquirimos un conocimiento tan específico y tan profundo que puede repercutir positivamente en otros clientes, sobre todo si pertenecen al mismo sector.

CUMPLIMIENTO EN TODOS LOS FRENTES

Hoy día la actividad de Ciberseguridad está íntimamente ligada al cumplimiento normativo. Las organizaciones están dotadas de una normativa interna de Ciberseguridad de obligado cumplimiento por parte de toda la entidad, a las que se añaden las leyes y regulaciones externas. En el caso de España nos encontramos la Ley Orgánica de Protección de Datos (LOPD) o la Ley de Protección de Infraestructuras Críticas (LPIC), por mencionar algunas, y en algunos sectores aplica regulación específica, como las exigencias del Banco Central Europeo (BCE) en las entidades financieras y de crédito, o el Esquema Nacional de Seguridad (ENS) en las administraciones públicas españolas.

Todo apunta a que en 2018 habrá un punto de inflexión en la aplicación de legislación y regulación que incorpora Ciberseguridad, a través del GDPR (*General Data Protection Regulation*) y de la Directiva NIS (*Network and Information Security*), que se unen o sobrepasan algunas de las leyes anteriormente mencionadas. El GDPR está acaparando todo el foco de atención, debido a que afecta de forma obligatoria a prácticamente cualquier organización y su cumplimiento se antoja complejo.

Este escenario de "sobrecumplimiento" es bastante familiar para empresas como GMV, dado que no es la primera (ni la última) de las leyes y regulaciones que abordamos, tanto como propios afectados como ayudando a nuestros clientes. En el conjunto de leyes ya consolidadas hemos aportado nuestros servicios para elaborar el análisis de riesgos, establecer un plan de adecuación, implementar las medidas de Ciberseguridad exigibles y demostrar el cumplimiento posteriormente.

¿Qué nos depara el futuro?

Están ocurriendo ciertas cosas que nos permite aventurarnos a predecir el futuro próximo de la Ciberseguridad. Hay varios datos que debemos tener en cuenta. Por ejemplo que el INCIBE (Instituto Nacional de Ciberseguridad) gestionó 115.000 incidentes en el 2016 (130% más que en el 2015); y una vez sufrido un incidente el 90% de las organizaciones mejoran sus procesos de seguridad y sus tecnologías de protección en idéntica proporción, según el "*Cisco 2017 Annual Cybersecurity Report*"; o que IDC en su "*2017 Global Security Product & Service Predictions*", establece que para el 2019 el 75% de los fabricantes de dispositivos IoT (Internet of Things) mejorarán las capacidades de seguridad y privacidad, o que para el 2018 el 70% de las infraestructuras de Ciberseguridad desplegadas incluirán inteligencia artificial y analítica de datos para mejorar su gestión.

A nivel contextual, el escenario IoT presenta todo un reto para protegerlo

LA OPINIÓN DE LOS EXPERTOS

¿ESTAMOS PREPARADOS ANTE LOS CIBERATAQUES O SE TRATA DE UNA ASIGNATURA PENDIENTE? ÉSTA Y OTRAS CUESTIONES SON LAS QUE HEMOS PLANTEADO A VARIOS EXPERTOS.

MARIA JOSÉ GARCIA
Directora de Tecnologías de la Información - Universidad Autónoma de Madrid (UAM)

¿Qué papel juega la Ciberseguridad dentro de su organización?

La Universidad Autónoma de Madrid (UAM), como Administración Pública, está sujeta al cumplimiento del Real Decreto 3/2010 por el que se regula el Esquema Nacional de Seguridad. Ya tan solo por el cumplimiento normativo, hemos de tener muy presente la Ciberseguridad, pero es que además, este asunto es de crítica importancia para asegurar la actividad diaria de la universidad, donde confluyen cada día una media de 50.000 usuarios, con perfiles y patrones de conducta en las redes muy variados. A eso hay que añadir que los estudiantes y los investigadores visitantes de otras universidades, traen consigo sus propios equipos que han de conectar a nuestra red, lo que añade otra capa más de incertidumbre en lo que se refiere a seguridad.

Somos conscientes de la importancia que tiene para la protección de los usuarios mantener el software actualizado, distribuyendo lo antes posible las últimas actualizaciones. En ese sentido, la UAM se encontró protegida frente al famoso ataque del virus WannaCry, pues la actualización de Microsoft que lo protegía ya se encontraba instalada en los equipos de docentes y personal de administración y servicios.

¿A qué se debe el incremento de las ciberamenazas y cómo lo están viviendo?

A lo largo del último año, cabe destacar que hemos detectado un incremento tremendo del trafico malicioso, escaneos de red y en concreto los relacionados con la BotNet Mirai y similares, afectando a los dispositivos del Internet de las cosas (IoT). Como dato ilustrativo, el 80-85% de las conexiones que nos llegan de Internet están siendo descartadas por nuestras medidas de protección.

Por otra parte, también notamos como los ataques de DDoS muestran un incremento preocupante, aunque hasta el momento nos han afectado mínimamente. Pero hay que tener en cuenta que con el "abaratamiento" de las infraestructuras por parte de los atacantes, es cada vez más fácil y se requieren menos medios para realizarlos.

¿Qué tendencias generales prevén?

El aumento de servicios digitales a través de la Administración Electrónica, hace imprescindible securizar los servicios implementando normativas específicas de seguridad.

En esa línea, la UAM aprobó en el año 2015 la Política de Seguridad de la Información, y poco a poco se van aprobando en Consejo de Gobierno normativas generales relativas a la seguridad.

También hemos realizado recientemente el primer Análisis de Impacto (BIA) en los servicios críticos, de modo que actualmente nos encontramos en la fase de estimación de los recursos necesarios para asegurar el tiempo objetivo de recuperación. Por otra parte, continuaremos desarrollando normativas enmarcadas en el ENS.

Por último, otro punto que hemos de reforzar es la formación a nuestros usuarios en temas de seguridad informática. Los

adecuadamente. Y hay que abordarlo desde un punto de vista global, empezando por la seguridad de los propios dispositivos (preferiblemente que venga de fábrica), siguiendo por la conectividad (con especial interés en la nube) y terminando en los sistemas finales que recogen todos los datos generados o que sirvan de plataformas de gestión (los datos se considera lo más valioso de todo).

A nivel tecnológico, podremos aprovecharnos de todos los avances en inteligencia artificial y aprendizaje para aplicarlos en nuevos algoritmos de analítica de datos desde la perspectiva de Ciberseguridad. Nos permite detectar comportamientos sospechosos nada evidentes en este momento, anticiparnos a futuros problemas y ser más eficientes en la gestión de los recursos.

A nivel de amenazas, seguiremos viendo muchos casos de chantaje, más conocido como ransomware, ya sea sofisticado o no. En este momento a los chantajistas les sale a cuenta porque la inversión necesaria para perpetrar el ataque es mínima, con gran impacto potencial y con probabilidades mínimas de ser descubiertos. Como ha pasado anteriormente (por ejemplo, con el spam de la primera década del siglo), es muy probable que la lucha contra el ransomware termine exterminándolo, o mutando a otro tipo de ataque, o simplemente que pase de moda.

últimos incidentes han sido tan populares que, en ese sentido, nos están ayudando a concienciar al Equipo de Gobierno respecto a la importancia de establecer normativas de Ciberseguridad, pero es igual de importante, cuando no más, que nuestros usuarios entiendan las medidas adoptadas y podamos contar de buen grado con su colaboración.

RAMÓN ORTIZ
Responsable de Seguridad - Mediaset

¿Qué papel juega la Ciberseguridad dentro de su organización?
Se constata el paso de un papel tradicionalmente reactivo en cuanto a la Ciberseguridad, para posicionarse como elemento necesario, previo y transversal en proyectos de transformación digital, de ingeniería y desarrollo de aplicaciones; en operaciones de sistemas, así como iniciativas diferenciadas de negocio.

En tanto que la tecnología es factor relevante, diferencial, e imprescindible en el negocio de Mediaset, las medidas y controles de Seguridad a adoptar son requeridos como garantía de integridad, disponibilidad y confidencialidad (+agilidad) de los activos de información y de los Servicios que presta la compañía y como un método eficaz de obtener y mantener confianza en los servicios y en la imagen del grupo Mediaset para la Audiencia de nuestros canales de TV, de los Usuarios de nuestros sites de internet y de cara a los Clientes y Anunciantes.

¿A qué se debe el incremento de las Ciberamenazas y cómo lo están viviendo?
Es evidente que cada año aumenta el número, variedad y gravedad de los ataques, así como las capacidades de los atacantes. Este incremento y perfeccionamiento de los ataques e incidentes no tiene de momento una explicación concluyente ni comúnmente aceptada.

De ser ciertas algunas de las explicaciones, en el sentido de la divulgación a entornos de ciberdelincuencia de determinadas capacidades y técnicas hasta ahora únicamente al alcance de agencias de gobiernos, la situación a la que deben enfrentarse las organizaciones, independientemente de su tamaño y recursos, es extremadamente preocupante y obliga a esfuerzos continuos de actualización y revisión de las medidas de prevención y control.

¿Qué tendencias generales prevén?
Ante el complicado entorno mencionado, las previsiones generales resultan similares a las que percibimos en Mediaset.

Alerta ante malware. Trabajar constantemente en configuración avanzada de las herramientas antimalware, explorar el uso de técnicas de análisis de comportamiento.

Mejoras en la Gestión de dispositivos Móviles. Hacer converger en la medida de lo posible las mismas medidas de seguridad en los dispositivos móviles que en los equipos clientes tradicionales. Es decir hacer del MDM no sólo una herramienta de gestión sino también de protección. Evitar traspaso de información entre aplicaciones personales y profesionales que conviven en el mismo dispositivo móvil.

Crear Conciencia. Por medio de adecuados planes de formación, concienciar a empleados y directivos de la relevancia de la Ciberseguridad en Mediaset, y de su papel activo cuando adoptan conductas responsables, en el incremento de la Seguridad. Compromiso de Mediaset con la Sociedad en divulgar aspectos de privacidad y seguridad.

Seguridad en entornos cloud. Adoptar los controles de acceso, monitorización y diseño de arquitectura análogamente al diseño de los entornos corporativos on premise, de modo que la Seguridad en ambos entornos sea equivalente. Adopción de prácticas y herramientas de control de utilización y consumo de recursos desplegados como control adicional de las plataformas alojadas en la nube.

Normativa. A la normativa ya vigente, se van a añadir nuevos requerimientos regulatorios; cada entidad, en función de su sector, se verá impactada en mayor o menor medida por nuevas normas que inciden en aspectos de Seguridad.

RAÚL
HERBOSA
Director Departamento de Sistemas - GMV

¿Qué papel juega la Ciberseguridad dentro de su organización?

En este mundo tan competitivo, todos nos centramos en nuestro trabajo directo y en el día a día, dejando el tema de la Ciberseguridad en un segundo plano, en muchos casos delegado al departamento de IT; "es su trabajo". En otras ocasiones, erróneamente se plantea el problema en términos de responsabilidad; "en caso de ataque, ¿tengo mis espaldas cubiertas?, ¿puedo tener alguna responsabilidad sobre las consecuencias?"

Evidentemente estos planteamientos son erróneos desde todo punto de vista, siendo un problema de todos y en el que todos, en la medida de nuestras posibilidades, debemos aportar para mantener un nivel adecuado de protección, ya sea concienciando a nuestro entorno en las buenas prácticas como medida de prevención, ya sea en nuestras propias actuaciones cotidianas. Lamentablemente en este tema la mejor concienciación se produce por un incidente concreto o por uno generalizado que tiene gran repercusión en los medios de comunicación y que dispara todas las alarmas.

En GMV tenemos una concienciación adicional debida a que la Ciberseguridad es una parte importante de nuestro negocio. Esto supone que no nos podemos permitir el lujo de lamentar no haber hecho lo suficiente para gestionar el riesgo y tener preparados nuestros sistemas de información ante posibles ataques en la medida de lo posible.

¿A qué se debe el incremento de las ciberamenazas y cómo lo están viviendo?

En un mundo tan globalizado como el actual y en el que vemos tantos intereses económicos cruzados, no es descabellado pensar en que las futuras "guerras" que puedan producirse sean a través de ciberataques que hagan tambalear uno u otro gobierno de forma remota y sin necesidad de arriesgar vidas humanas. Por ahora lo que estamos viendo es la tendencia al alza desmesurada año tras año en el número de ataques y el número de ciberamenazas existentes.

En nuestro departamento tratamos este tema desde la prudencia, siempre teniendo en cuenta la máxima "no existe la seguridad perfecta". Esto hace que no bajemos la guardia en ningún momento, además de evitar una actitud de arrogancia por no haber tenido ninguna infección/incidente en los últimos ataques masivos tan populares.

¿Qué tendencias generales prevén?

La tendencia de los últimos años nos indica que en un futuro los ataques y las ciberamenazas se verán incrementados. En este sentido, no debemos ser alarmistas, pero tampoco quedarnos con los brazos cruzados, esperando que el destino no nos depare ser las siguientes víctimas de las últimas amenazas respecto a intereses económicos, políticos, religiosos, etc.

La aparición y auge de nuevas tecnologías como el IoT, dispositivos móviles, redes Wi-Fi o soluciones Cloud hacen más que nunca necesario definir nuestro propio proceso de Ciberdefensa que permita mantenernos en un nivel de alerta y de seguridad razonable y adaptado a cada negocio para poder continuar con los procesos productivos asociados a nuestras empresas de forma continua.

Equipo del Departamento de Sistemas de GMV

ALBERTO HERNÁNDEZ

DIRECTOR GENERAL DE INSTITUTO NACIONAL DE CIBERSEGURIDAD DE ESPAÑA (INCIBE)

EL INSTITUTO NACIONAL DE CIBERSEGURIDAD ES UNA ENTIDAD PÚBLICA ADSCRITA AL MINISTERIO DE ENERGÍA TURISMO Y AGENDA DIGITAL A TRAVÉS DE LA SECRETARIA DE ESTADO PARA LA SOCIEDAD DE LA INFORMACIÓN Y LA AGENDA DIGITAL. SU MISIÓN FUNDAMENTAL ES PRESTAR SERVICIOS PÚBLICOS DE CIBERSEGURIDAD A LOS CIUDADANOS Y AL SECTOR PRIVADO EN ESPAÑA, CON ATENCIÓN ESPECIAL A LOS OPERADORES PRIVADOS DE INFRAESTRUCTURAS CRÍTICAS GRACIAS A UN CONVENIO DE COLABORACIÓN CON EL MINISTERIO DEL INTERIOR, A TRAVÉS DE SU CENTRO NACIONAL DE PROTECCIÓN DE INFRAESTRUCTURAS CRÍTICAS (CNPIC) Y FRUTO DEL CUAL SE CONSTITUYE UN CERT (CENTRO DE RESPUESTA ANTE INCIDENTES). SU DIRECTOR GENERAL, ALBERTO HERNÁNDEZ, PROFUNDIZA SOBRE EL TRABAJO QUE REALIZAN, ASÍ COMO SOBRE LOS RETOS A LOS QUE SE ENFRENTAN COMO "GUARDIANES" DE LA CIBERSEGURIDAD.

¿CUÁLES SON LOS PRINCIPALES ÁMBITOS EN LOS QUE CENTRÁIS VUESTRA ACTIVIDAD?

El primer enfoque en el que trabajamos, de servicio público, se basa en la prevención y en la concienciación de ciudadanos y empresas sobre el uso seguro de las tecnologías, humanizando la Ciberseguridad.

El segundo ámbito de actuación de INCIBE se centra en identificar las capacidades para detectar de forma proactiva ciberincidentes o ciberataques que sucedan en España y que afecten a sus ciudadanos y a su sector privado para localizarlos, analizarlos y ponerlos en conocimiento de los afectados.

¿CÓMO LOS ABORDÁIS?

La aproximación de INCIBE es muy blanca ya que no monitorizamos la actividad de ciudadanos o empresas. En el marco de acuerdos de colaboración nacionales e internacionales, establecemos mecanismos de intercambio de información ya sea a través de empresas de Ciberseguridad de ámbito internacional o mediante la adquisición de fuentes de información, lo que nos permite cada año analizar más de 10 millones de eventos de información relacionados con incidentes en España y detectar del orden de 100.000 redes infectadas diarias en nuestro país. En INCIBE somos un referente internacional en servicios antibots, un servicio muy novedoso a nivel mundial, donde gracias a la colaboración con los ISPs (proveedores de internet como las operadoras de telecomunicaciones) podemos identificar de forma proactiva las IPs de los usuarios infectadas por algún tipo de malware. Detectamos, analizamos lo que está pasando, cuál es el origen del problema, en que consiste el incidente y lo comunicamos. Esto recalca la necesidad de que la Ciberseguridad tenemos que hacerla entre todos, la colaboración entre el ámbito público y el sector privado es fundamental en la protección de nuestros ciudadanos y empresas.

ESTE ES UN PUNTO DELICADO, YA QUE SE HABLA DE LA COMPARTICIÓN DE INFORMACIÓN ¿QUÉ MEDIDAS PREVÉS PUEDAN IR MÁS LEJOS EN LA OBLIGACIÓN DE QUE EL SECTOR PRIVADO COMPARTA CON EL PÚBLICO INFORMACIÓN PARA CONTRIBUIR A LA LUCHA COLECTIVA CONTRA EL CIBERDELITO?

En la transposición de la directiva de seguridad en redes y sistemas de información de la Unión Europea se establece para las empresas que gestionen servicios esenciales la obligatoriedad de notificar los incidentes de seguridad. Resulta muy importante trabajar en la alerta temprana, más que en la obligatoriedad debemos centrarnos en entender los beneficios de la prevención. Si comparamos los incidentes que hemos gestionado en 2016 (115.000) y en 2015 (50.000), observamos que este significativo incremento se debe a tres factores: a la mayor capacidad de detección como consecuencia de una mayor inversión, a una mejor comunicación entre empresas y ciudadanos y, en tercer lugar, al incremento global de incidentes. Estamos notando un aumento en la cantidad y el tipo de información que el sector privado, por el beneficio que le reporta, nos traslada.

Y BAJO EL PUNTO DE VISTA DE LAS ENTIDADES PRIVADAS, QUE NO SEAN OPERADORES DE INFRAESTRUCTURAS CRÍTICAS PARA LOS QUE LA SITUACIÓN ESTÁ MUY REGULADA, ¿CÓMO RECOMENDARÍAS QUE SE ARTICULARA LA RELACIÓN CON INCIBE? ¿CÓMO LES PROPONÉIS QUE SE ACERQUEN A VOSOTROS?

Desde un punto de vista preventivo, conectándose a la web e involucrándose en nuestros proyectos. Por ejemplo, ofrecemos un kit de concienciación, que permite a cualquier empresa acceder a un plan de concienciación y a todos los materiales necesarios para aplicarlo. Disponemos de herramientas muy sencillas para empezar a conocer los riesgos de la organización, desde elementos de gaming con itinerarios interactivos para los empleados hasta un juego online donde contrastar los conocimientos.

> LA COLABORACIÓN ENTRE EL ÁMBITO PÚBLICO Y EL SECTOR PRIVADO ES FUNDAMENTAL EN LA PROTECCIÓN DE NUESTROS CIUDADANOS Y EMPRESAS

En caso de que hayan sufrido algún ciberincidente se abren dos vías. La primera es la denuncia a las fuerzas de seguridad del estado y la segunda a través del CERT de Seguridad e Industria que operamos desde INCIBE. Podemos ayudar en el análisis del problema y darles una respuesta En los ataques ransomware que ahora están todos los días en los medios de comunicación, que ya sucedían antes aunque no saliesen, disponemos de un servicio público de descifrado con una tasa de éxito superior al 80% y de forma gratuita.

Y por último, implicándose en las actividades desarrolladas desde INCIBE

en colaboración con empresas de Ciberseguridad, que incluyen acciones de concienciación y otras iniciativas gratuitas por todo el territorio nacional para acercar la Ciberseguridad a todos los empresarios.

HAS MENCIONADO LA COLABORACIÓN CON LA INDUSTRIA DE CIBERSEGURIDAD NACIONAL, ¿CÓMO ESTÁ ARTICULADA?

Se ha constituido lo que denominamos un polo tecnológico de Ciberseguridad, que es un espacio donde buscamos sinergias entre las inquietudes de la industria y la acción de los organismos públicos. Desde INCIBE apoyamos a la industria nacional en la internacionalización y la mejora de su competitividad. Como entidad dependiente del Ministerio de Energía, Turismo y Agenda Digital estamos muy interesados en el desarrollo industrial de nuestro país y en la generación de puestos de trabajo. Por lo tanto, trabajamos conjuntamente con la industria de Ciberseguridad identificando actividades que permitan mejorar la competitividad de nuestra industria aumentando su internacionalización. Disponemos de un Plan de Confianza en el Ámbito Digital (derivado de la Agenda Digital para España), para identificar la demanda de Ciberseguridad de las empresas en los próximos años, de forma que la industria del sector pueda desarrollar productos y servicios adaptados, y a su vez, trabajar con los centros de I+D+i nacionales orientados a la Ciberseguridad. Dentro de este Plan, INCIBE ha liderado la constitución de una Red de Centros de Excelencia de I+D+i, con el objetivo de aglutinar los esfuerzos de este ecosistema existentes en la actualidad y dirigir su actividad de forma coordinada a través de un futuro plan director alineado con la estrategia europea y las necesidades reales de la industria y los usuarios finales. Otra de las actividades es la celebración anual de las jornadas nacionales de I+D+i en Ciberseguridad "JNIC", que suponen un punto de encuentro entre los diversos actores que trabajan en el ámbito de la investigación en Ciberseguridad (universidades, centros tecnológicos y de investigación, empresas, y administración pública) donde puedan intercambiar conocimiento y experiencias con el objetivo común de potenciar la investigación en el ámbito de la Ciberseguridad a nivel nacional. Otra forma de colaboración es favorecer en todo lo posible la generación de startups.

¿Y QUÉ OTRAS INSTITUCIONES, COMO ES EL CASO DEL CDTI, APOYAN ESTE TIPO DE INICIATIVAS? ¿TENÉIS SUSCRITO ALGÚN ACUERDO QUE APOYE EL EMPRENDIMIENTO?

Otros organismos públicos que trabajan conjuntamente con nosotros son CDTI, el ICEX (internacionalización) y ENISA España, con los que apoyamos el emprendimiento, la internacionalización y la generación de startups. También está presente la industria durante las diferentes fases del proceso de aceleración, bien en los comités asesores, en los comités científicos o en el propio tribunal que selecciona los proyectos, a través de iniciativas como "Cyber-emprende" o "Cybersecurity Ventures", una aceleradora internacional que constituimos junto con la Junta de Castilla y León y el Ayuntamiento de León. Esta línea de trabajo de INCIBE no tendría sentido sin la colaboración de la propia industria de Ciberseguridad. Recientemente, para abordar la crisis de WannaCry o petya, INCIBE trabajó conjuntamente con el Centro Criptológico Nacional, el Mando conjunto de Ciberdefensa, la Guardia Civil, Policía, unidades especializadas de investigación, pero también con representantes de la industria de la Ciberseguridad. Durante esos días se establecieron mecanismos de intercambio de información en tiempo real, consiguiendo que, gracias a esta colaboración, el impacto en España fuese limitado.

¿CUÁL SERÍA TU FOTO DE LA INDUSTRIA NACIONAL DE CIBERSEGURIDAD EN ESTE MOMENTO? ¿CUÁL ES SU NIVEL DE DESARROLLO EN COMPARACIÓN CON OTROS PAÍSES Y CON LA INDUSTRIA TIC EN GENERAL?

Hemos identificado cerca de 130 a 140 empresas que llamamos "Pure Players" en Ciberseguridad, es decir, empresas que tienen productos/servicios o una unidad de negocio de Ciberseguridad en España.

Son todas empresas que operan en España, incluidas multinacionales. Creemos que todavía son escasas y de tamaño heterogéneo, predominando las pequeñas empresas. En comparación

WANNACRY HA SUPUESTO PARA NUESTRO PAÍS UN ANTES Y UN DESPUÉS. AHORA PRÁCTICAMENTE LA TOTALIDAD DE LOS CIUDADANOS Y DE LOS EMPRESARIOS ESTÁN MÁS CONCIENCIADOS ACERCA DE LA IMPORTANCIA DE LA CIBERSEGURIDAD

con otros países, se trata de una industria pequeña, aunque ágil y eficiente, y compite en el mercado internacional.

¿CÓMO VES LA EVOLUCIÓN DE LAS EMPRESAS DEL SECTOR DE LA CIBERSEGURIDAD?

Nuestros estudios sobre tendencias de Ciberseguridad indican que las grandes empresas o las ya posicionadas seguirán creciendo, a la vez que existen oportunidades para la generación de startups. La agilidad propia de emprendedores y empresas pequeñas permite a éstas acceder a nichos o mercados que las empresas grandes ignoran. Creemos que hay oportunidades para ambas, de hecho nuestro estudio de tendencias del pasado año concluye que el mercado de Ciberseguridad estará liderado por grandes empresas con un espacio importante para la pequeña y mediana basado en un factor fundamental en el ámbito TIC: la innovación disruptiva. Hemos visto cómo empresas que nacieron en un garaje con una idea disruptiva pronto dieron lugar a multinacionales. Creemos que este factor va a resultar diferenciador durante muchos años, abriendo posibilidades a la aparición de pequeñas empresas y permitiendo a las ya asentadas participar de sus proyectos e incorporar nuevos productos y servicios.

¿CONSIDERAS QUE EL ESTADO ESPAÑOL DEDICA LOS RECURSOS NECESARIOS EN CIBERSEGURIDAD?

En los presupuestos generales del Estado hay una partida suficiente para el contexto actual. Como dato positivo diría que el presupuesto de INCIBE ha experimentado un incremento porcentual importante, lo que demuestra la apuesta por el proyecto. ¿Debemos invertir más? Desde un punto de vista global, se requiere dinero para sanidad, para educación… Lo que estamos observando es un incremento del presupuesto de Ciberseguridad acorde con los recursos de España.

LA FIGURA DE INCIBE NO PARECE QUE TENGA MUCHAS RÉPLICAS EN OTROS PAÍSES, ¿CONOCE PRECEDENTES DE INSTITUCIONES SIMILARES QUE JUEGUEN UN PAPEL DE APOYO INSTITUCIONAL A LA CIBERSEGURIDAD, NO SOLO PÚBLICA SINO PRIVADA?

Un valor diferencial de INCIBE es su proyección internacional con doble objetivo: establecer mecanismos de colaboración para el intercambio de información, y proyectar una imagen de fuerte posicionamiento de nuestra industria. Quizás este segundo objetivo resulte más diferenciador frente a otras iniciativas a nivel europeo, limitadas a meras agencias centradas en la seguridad del país. En Latinoamérica, como expertos internacionales apoyamos el desarrollo de las estrategias de Ciberseguridad nacional de diversos países que en muchos casos están adoptando INCIBE como modelo.

¿CÓMO VES LA TRANSFORMACIÓN DIGITAL QUE ESTÁ PROTAGONIZANDO LA CUARTA REVOLUCIÓN INDUSTRIAL? ¿ESTÁN PREPARADOS ESTOS SECTORES PARA ASUMIR EL RETO QUE SUPONE LA CONEXIÓN DE SUS PRODUCTOS Y SERVICIOS EN TÉRMINOS DE CIBERSEGURIDAD?

La transformación digital está resultando muy rápida, y quizá sin demasiada consideración hacia la Ciberseguridad. WannaCry ha supuesto para nuestro país un antes y un después. Ahora prácticamente la totalidad de los ciudadanos y de los empresarios están más concienciados acerca de la importancia de la Ciberseguridad, valorándola como una inversión.

¿CUÁL TE PARECE QUE ES LA BARRERA MÁS IMPORTANTE PARA QUE TODAS ESTAS INDUSTRIAS QUE SE ESTÁN DIGITALIZANDO ASUMAN LA CIBERSEGURIDAD COMO IMPRESCINDIBLE PARA SU ACTIVIDAD?

Evidentemente existe una barrera económica porque supone un coste, pero éste se debe valorar en función de los beneficios. Creo que estamos en mejor situación que antes, que los empresarios empiezan a entender que es una necesidad para su negocio.

SI HABLAMOS DE TRANSFORMACIÓN DIGITAL, UN ELEMENTO CLAVE Y QUIZÁ NO RESUELTO ES LA

DISPONIBILIDAD DE TALENTO DIGITAL. EN CIBERSEGURIDAD ¿CÓMO ESTÁ LA SITUACIÓN?

Existen estudios sobre la demanda no satisfecha de profesionales de ww en Europa, que es considerable. En 2014 se anunciaba para 2017 casi 700.000 puestos de trabajo no cubiertos en el ámbito de las tecnologías de la Ciberseguridad en Europa, y para 2020 se estima que esta cifra ronde el millón de puestos de trabajo. En España tenemos entre 5000 y 6000 profesionales trabajando en Ciberseguridad, por lo que la demanda es más pequeña pero sigue existiendo un gap importante sobre el que tenemos que trabajar. En el evento anual Cybercamp que organizamos con el objetivo de acercar la Ciberseguridad a padres, niños y jóvenes talentos, el pasado año asistieron en León cerca de 20.000 personas, se ofertaron más de 2.200 puestos de trabajo e iniciativas formativas gratuitas y sólo recibimos escasos 900 curriculums. Esto indica que hay un gap muy grande, y que es necesario implementar programas para promover el talento entre jóvenes de 14, 15, 16 años. Desde INCIBE estamos desarrollando iniciativas para promover el interés entre los jóvenes por dedicarse a este sector, identificar talento y establecer el contacto con las empresas. Queda mucho por hacer, pero creo que vamos por buen camino. Como ejemplo, el año pasado en el campeonato *European Cyber Security Challenges* el equipo español, formado por 10 jóvenes talentos identificados en Cybercamp, fue el campeón de Europa. Esto demuestra que en España hay talento y que las actividades que estamos llevando a cabo están dando sus frutos.

Y PARA LAS MUJERES, ¿IMPULSÁIS ACCIONES QUE FOMENTEN LA IGUALDAD?

Entre los objetivos fijados en el marco de la nueva agenda digital para España figura trabajar en la diversidad de género para que en este sector las mujeres tengan el papel que les corresponde. Este año organizamos en colaboración con la Organización de Estados Americanos (OEA) el "I Foro Internacional de Género y Ciberseguridad" por un mundo digital más inclusivo, donde se analizó la situación actual y problemática de género tanto a nivel nacional como internacional en el sector de la Ciberseguridad. La idea es seguir trabajando para definir y desarrollar estrategias que permitan esa diversidad de género en el ámbito de la Ciberseguridad.

VOLVIENDO AL ESCENARIO DE RANSOMWARE. HACE POCO MÁS DE UN AÑO, EN REINO UNIDO Y EEUU HAN TENIDO LUGAR ATAQUES EN EL SECTOR DE SALUD. ¿POR QUÉ CREES QUE SE ATACÓ EN PARTICULAR ESE SECTOR? ¿PIENSAS QUE EN NUESTRO PAÍS HAY SECTORES PARTICULARMENTE MÁS EXPUESTOS?

La radiografía de los incidentes en España muestra mayor incidencia en aquellos sectores tecnológicamente más avanzados, con un incremento en sectores que hace tres años apenas registraban incidentes y que están invirtiendo en tecnología y, por lo tanto, resultan más sensibles a ciberataques. Estamos trabajando intensamente en la Ciberseguridad de los sistemas de control industrial, tratando de que incorporen la Ciberseguridad desde su diseño y accedan a Internet de forma segura.

Las micropymes, mayoritarias en España y que utilizan cada vez más tecnología, suelen carecer del nivel de seguridad adecuado, porque no manejan el concepto o no sienten la necesidad. Por lo tanto, debemos incidir en la necesidad de humanizar la Ciberseguridad y trabajar todos, no solamente INCIBE, en explicar que con poca inversión se pueden alcanzar niveles de protección altos.

¿CÓMO ESTAMOS SITUADOS EN I+D EN CIBERSEGURIDAD EN ESPAÑA?

Si hablamos en términos de inversión en I+D+i encontramos países de nuestro tamaño situados por encima y por debajo de nosotros. Respecto a países con mayor presupuesto (Estados Unidos, Reino Unido) nos encontramos bastante por debajo, si bien España destaca en algunos aspectos: somos eficientes y tenemos muy buen talento. Hemos de seguir ese camino, apoyando el talento y fomentando que nuestras empresas desarrollen y vendan fuera sus ideas.

GMV LLEVA TRABAJANDO CON INCIBE DESDE HACE 10 AÑOS, ¿QUÉ DESTACARÍAS DE LA COLABORACIÓN QUE VENIMOS MANTENIENDO?

Creemos que habéis realizado un trabajo excelente, avalado por muchos años de colaboración en proyectos esenciales para nuestra actividad. Vuestro perfil, muy orientado al exterior, constituye un ejemplo positivo de compañía con capacidad para satisfacer necesidades internas y para trabajar intensamente hacia fuera.

Luis Fernando Álvarez-Gascón, Director General de GMV Secure e-Solutions y Alberto Hernández, Director General de INCIBE

En la siguiente fase del proyecto GMV contribuirá con el inicio de la transmisión de una señal SBAS de segunda generación. Está señal será capaz de proveer a los usuarios GNSS de un doble servicio SBAS y PPP, incluyendo la aumentación tanto de satélites GPS como Galileo

GMV contribuye a la primera transmisión de una señal SBAS sobre Australia y Nueva Zelanda

Recientemente GMV ha contribuido a la primera transmisión de una señal SBAS a través de un satélite geoestacionario sobre Australia y Nueva Zelanda. Los Sistemas de Aumentación Basados en Satélites (SBAS por sus siglas en inglés) mejoran la precisión del posicionamiento y la integridad de los satélites GPS. Estos sistemas ya se han desplegado en Estados Unidos (WAAS), Europa (EGNOS), India (GAGAN) y Japón (MSAS) y existen iniciativas similares en marcha en otros países, como China (SNAS), Rusia (SDCM) y Corea del Sur (KASS).

Esta primera transmisión se realiza como parte de la estrategia de los gobiernos australiano y neozelandés para el desarrollo de la infraestructura de posicionamiento en la región de Australasia. El proyecto tiene una duración de 2 años y está coordinado por Geoscience Australia (GA) y el Centro Cooperativo de Investigación para la Información Espacial de Australia y Nueva Zelanda (CRCSI, por sus siglas en inglés). GMV, Lockheed Martin e Inmarsat colaboran en el proyecto aportando la infraestructura de generación y transmisión de los mensajes SBAS.

El objetivo del proyecto es mostrar los posibles beneficios de las tecnologías de navegación por satélite incluyendo servidos de integridad y gran precisión. Para ello, en los próximos meses se realizaran diversas experimentaciones y pruebas haciendo uso de la señal SBAS en diversos sectores como la agricultura, construcción, minería o transporte entre otros.

Para el desarrollo de la infraestructura, a principios de año Geoscience Australia (GA) seleccionó a GMV para el suministro de los elementos de procesado a cargo de la generación de los mensajes SBAS y los equipos de usuario, Lockheed Martin para el enlace de señal con el satélite geoestacionario, e Inmarsat como proveedor del satélite a cargo de transmitir la señal.

Para llevar a cabo este hito, en mayo, dos ingenieros de GMV se trasladaron a las instalaciones de Lockheed Martin en Uralla, Nueva Gales del Sur (Australia) para participar en la instalación e integración del sistema. Poco después, a principios de junio, Geoscience Australia junto con las autoridades de aviación australianas autorizaron el comienzo de la transmisión.

En la siguiente fase del proyecto GMV contribuirá con el inicio de la transmisión de una señal SBAS de segunda generación. Está señal será capaz de proveer a los usuarios GNSS de un doble servicio SBAS y PPP, incluyendo la aumentación tanto de satélites GPS como Galileo.

GMV, miembro del consorcio que suministrará los servicios Copernicus de soporte a acciones exteriores de la UE

EGEOS, EMPRESA FORMADA POR TELESPAZIO (80%) Y LA AGENCIA ESPACIAL ITALIANA (20%), HA SUSCRITO CON EL CENTRO DE SATÉLITES DE LA UNIÓN EUROPEA (SATCEN) UN CONTRATO MARCO VALORADO EN 7,5 MILLONES DE EUROS, PARA EL SUMINISTRO DE LOS SERVICIOS COPERNICUS DE SEGURIDAD, EN EL ÁREA DE SOPORTE A ACCIONES EXTERIORES (SEA). ESTE SERVICIO TIENE COMO OBJETIVO PROPORCIONAR INFORMACIÓN GEOESPACIAL DE ÁREAS CRÍTICAS REMOTAS Y DE DIFÍCIL ACCESO, CON GRAN RIESGO PARA LA SEGURIDAD, AYUDANDO TAMBIÉN A TERCEROS PAÍSES A PREVENIR AMENAZAS GLOBALES Y TRANSREGIONALES CON EFECTO DESESTABILIZADOR

El contrato requiere analizar un gran número de imágenes de satélite bajo una producción de 24 horas al día. Para proveer los productos de valor añadido asociados, e-GEOS lidera un consorcio europeo formado por GMV, GAF, Telespazio Ibérica, Airbus DS, IABG y SIRS. GMV, como miembro de este potente equipo de operadores industriales, prestará los servicios operacionales de apoyo a la producción geoespacial en el ámbito de la acción externa de la Unión Europea.

El servicio de producción geoespacial consiste en servicios de análisis de imágenes de observación de la Tierra con una cartera consolidada de productos para diferentes niveles de intensidad de activación. El contrato estará operativo las 24 horas del día a partir de órdenes de activación emitidas por SatCen (*European Union Satellite Centre*), siempre y que se reciba una petición de los usuarios finales. De este modo, SatCen actuará como enlace entre usuarios e industria y valorará la calidad de los productos finales.

GMV ofrece dos centros de producción (España y Portugal) que realizarán evaluaciones internas de la calidad de los mapas como apoyo al proceso de toma de decisiones tácticas y estratégicas. GMV tiene capacidad para generar cualquier producto de la cartera de este servicio Copernicus y dará soporte a la dirección general del proyecto desempeñando la función de gestor de la calidad. Esta función se centrará en la evaluación offline de la calidad de los productos, en paralelo con el ejercicio de validación de SatCen, a fin de detectar fallos constantes causados por un flujo inadecuado del procesado. Los comentarios servirán para mejorar la cadena global y la calidad de los productos, reducir el número de reprocesados por baja calidad y consecuentemente, mejorar el tiempo de entrega. Además, GMV desarrollará un interfaz web para gestionar el alta y desarrollo de las órdenes de producción dando información detallada del proceso y de los consumos de recursos asociados.

El programa Copernicus espera alcanzar un sistema autónomo de observación de la Tierra a través de una red de satélites, una red de estaciones de medida en tierra y medios aerotransportados, así como la generación de servicios de información. El objetivo es observar el planeta desde todos los puntos de vista posibles para entender mejor los cambios que se producen y cómo influyen en nuestra vidas.

Por su parte, los servicios Copernicus se encargan de transformar los datos que recogen los satélites in situ, en información de valor añadido, gracias al procesamiento y análisis de los mismos, a su integración con otras fuentes y a la validación de resultados.

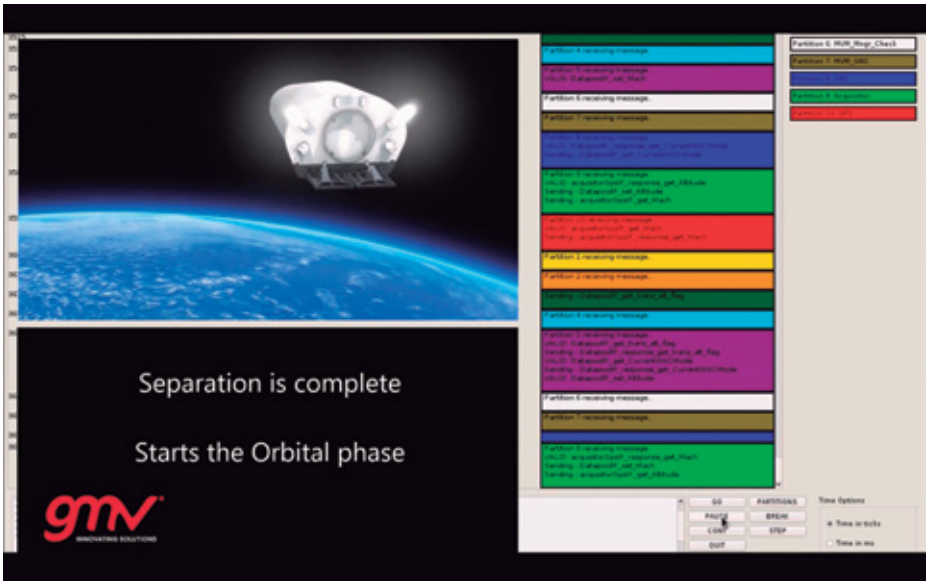
MORA-IMA combina los mayores objetivos tecnológicos relacionados con el software espacial embebido

LA AGENCIA ESPACIAL EUROPEA (ESA) HA CONFIADO DE NUEVO EN LA EXPERIENCIA DE GMV TANTO EN ARQUITECTURA DE REFERENCIA DE SOFTWARE EMBARCADO (OSRA) COMO EN AVIÓNICA MODULAR INTEGRADA (IMA). EL EQUIPO DIRIGIDO POR GMV EN PORTUGAL VA A DESARROLLAR UNA "IMPLANTACIÓN MULTI-NÚCLEO DE ARQUITECTURA DE REFERENCIA DE SOFTWARE EMBARCADO CON FUNCIONES DE IMA" (MORA-IMA)

OSRA es una solución única, consensuada y común para definir la arquitectura de los sistemas de software embarcados que permite lograr un proceso de desarrollo de software rápido y basado en modelos.

IMA, también conocido como segregación espacial y temporal (TSP), es un paradigma adoptado en numerosos sectores, que permite la ejecución de software muy crítico combinado con otro no crítico. Esta combinación de criticidad se consigue mediante el aislamiento (segregación) en el tiempo y en el espacio de las aplicaciones de software que componen el sistema de aviónica. Asimismo, IMA/TSP es una posible solución elegida para futuros ordenadores multi-núcleo dentro de una filosofía de asociación de núcleos procesadores a particiones.

MORA-IMA combinará por primera vez los tres objetivos tecnológicos principales de la ESA relacionados con el software espacial embebido



La finalidad de MORA-IMA consiste en mostrar la viabilidad y evaluar el desempeño de un proceso, unos instrumentos y unos elementos de construcción de extremo a extremo desde la especificación del nivel de aplicación utilizando el planteamiento OSRA para la implantación combinada de OSRA, TSP, multiprocesamiento simétrico (SMP) y multi-núcleo.

En otras palabras, MORA-IMA combinará por primera vez los tres objetivos tecnológicos principales de la ESA relacionados con el software espacial embebido. Dará lugar a un proceso de extremo a extremo comenzando por el diseño de software de alto nivel, pasando por una arquitectura completa de aviónica, sistemas y software utilizando el proceso OSRA, y terminará con la generación, creación y ejecución de códigos automáticos en un ordenador espacial multi-núcleo que aplique el paradigma IMA/TSP.

El caso de uso elegido para este estudio es la Misión de Referencia EagleEye de la ESA, la misión espacial virtual de la Agencia para pruebas de software, que se ha utilizado y se usa actualmente para probar y evaluar métodos, tecnologías e instrumentos destinados al desarrollo de misiones espaciales. EagleEye incluye un sistema de validación de software (SVF) completo y el software central (CSW) de un satélite debidamente instalado en el banco de pruebas de aviónica (ATB) de la ESA.

Eutelsat confía en GMV para sus próximas cuatro misiones

EUTELSAT HA VUELTO A CONFIAR A GMV LA IMPLEMENTACIÓN DEL CENTRO DE CONTROL (NEO-SCC), VERSIÓN PARA EUTELSAT DEL PRODUCTO DE GMV ***hifly®***, ASÍ COMO EL SISTEMA DE DINÁMICA DE VUELO BASADO EN ***focusGEO***, PARA SUS PRÓXIMAS CUATRO MISIONES

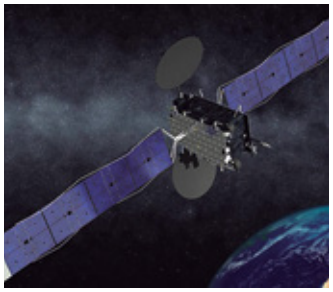
Actualmente Eutelsat es uno de los clientes de referencia de GMV y cuenta con sistemas desarrollados por GMV para el control de su flota de satélites al completo, entre los que destacan el sistema multisatélite de control de satélites ***hifly®***, y el sistema de dinámica de vuelo ***focusGEO***.

La sólida y larga relación entre GMV y Eutelsat, que se remonta a 1993 con la adjudicación del primer contrato, se ha forjado en gran medida por la dedicación de un gran número de personas que han puesto todo su empeño y su buen hacer para lograr unos resultados de gran calidad. Durante este periodo este equipo se ha ido renovando y ha logrado no sólo conservar ese espíritu de superación sino incrementar el número de desarrollos y actividades realizadas para Eutelsat.

Avant Project, como se ha denominado el proyecto, supone el primer desarrollo de GMV para Eutelsat que requiere la implementación casi en paralelo de cuatro nuevos satélites. Supone un reto tanto técnico como de gestión para el que se prevé el uso de sinergias de otros desarrollos de GMV tanto de la familia ***focus*** como ***hifly®***. Asimismo, en su hoja de ruta, el proyecto contempla el uso de metodologías ágiles de desarrollo con el objetivo de lograr una solución óptima en recursos de GMV y centrada en cumplir los objetivos operacionales, de calidad y funcionales requeridos por Eutelsat.

Avant Project se prolongará hasta principios de 2019 y dará soporte a las operaciones de Eutelsat para los siguientes cuatro satélites:

African broadband satellite de Thales Alenia Space y basado en la nueva plataforma Spacebus Neo que, al igual que Quantum, proporciona un protocolo de transmisión de telemetría y telecomando basado en el estándar PUS de la ESA. African brodband satélite será lanzado durante 2019.



Eutelsat 5 West B, primer satélite de Eutelsat del fabricante Orbital ATK con una plataforma GeoStar2 y una carga de pago de Airbus Defence and Space. Será lanzado igualmente durante el próximo 2018.

Eutelsat Quantum del fabricante Airbus Defence and Space (ADS) en UK con una plataforma fabricada por su filial Surrey Satellite Technology Ltd. (SSTL). Quatum es el primer satélite que posibilita una completa re-configuración a bordo.

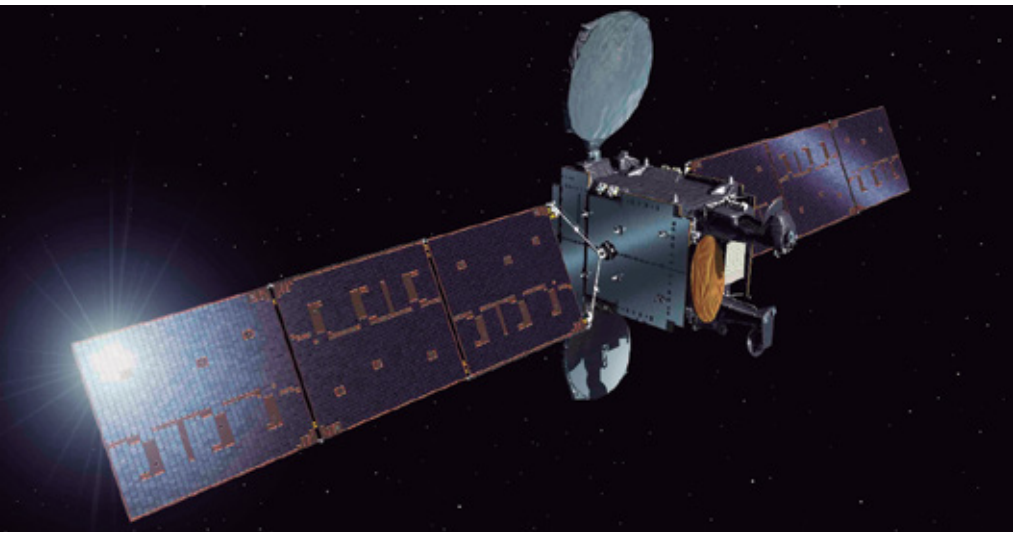
Eutelsat 7C de la plataforma Omega 3 de Space Systems Loral que será lanzado el tercer cuarto de 2018 para dar cobertura de ancho de banda a Europa, Africa, Oriente Medio y Turquía.

Comienza la fase operacional del satélite HISPASAT AG1

El día 2 de junio y tras la conclusión de la fase de "commissioning", el satélite Hispasat 36W-1 (AG1) fue oficialmente transferido al equipo de operaciones, un hito que marca el comienzo de la vida operacional del satélite.

Lanzado el 28 de enero, Hispasat AG1 es la primera misión de la plataforma SmallGEO, desarrollada por OHB System AG (Alemania) con la Agencia Espacial Europea e HISPASAT. El satélite incorpora una innovadora carga útil regenerativa RedSAT, que permitirá a HISPASAT utilizar de manera más ágil y eficiente la potencia del satélite, aumentando sustancialmente la capacidad de transmisión con la consiguiente reducción del coste de las comunicaciones.

Para poder dar soporte a los 20 transpondedores en banda Ku y hasta 3 en banda Ka, además de una innovadora antena activa de haces reconfigurables, GMV ha entregado también a Hispasat la última versión de sus herramientas de la familia Smart: ***smart rings*** como solución de GMV que permite buscar alternativas de configuración de la carga útil ante un fallo de algún componente de la misma y ***smart beams***, que ofrece al usuario control sobre las antenas del satélite tanto a nivel de configuración de apuntamiento como de comprobación, en un mapa 3D, del eje de las mismas.



Ambas herramientas están plenamente integradas tanto con el sistema multisatélite de control y monitorización, ***hifly®***, como con el sistema para las operaciones de dinámica de vuelo, ***focusGEO***, que GMV también ha suministrado. Además para este satélite, ***hifly®*** ha incorporado el soporte al nuevo modelo de definición de telemetría y telecomando de la ESA denominado PUS, nuevo estandard que ya está siendo incorporado por otros fabricantes en sus nuevos modelos de satélite.

HELLAS SAT 3 despega con éxito

El día 29 de junio, un cohete europeo Ariane 5 puso en órbita desde la base de Kurú, Hellas Sat 3, el nuevo satélite de telecomunicaciones de la flota de Hellas Sat, subsidiaria de Arabsat.

Hellas Sat 3 es un satélite compartido entre Hellas Sat e Inmarsat, que llevará a cabo dos misiones: Inmarsat desplegará una red integrada de telecomunicaciones para dar servicio de internet a los aviones en la zona europea, mientras que Hellasat ofrecerá sevicios de teledifusión directa y de telecomunicaciones a Europa, Oriente Medio y Norte de África sustituyendo y ampliando las capacidades de su predecesor, Hellas Sat 2, que ya se encuentra al final de su vida útil.

GMV ha desarrollado el sistema de dinámica de vuelo y el sistema de control y monitorización de Hellas Sat 3. Ambos sistemas, se han desarrollado sobre la base de las soluciones de GMV ***focusGEO*** y ***hifly®***. Ambas soluciones han sido integradas y desplegadas con éxito en un entorno virtual moderno y ecológico que utiliza servidores blade y vSphere. Además del software, GMV proporciona también formación, soporte y mantenimiento para los usuarios finales del sistema.

El lanzamiento de este satélite, así como su puesta en funcionamiento operacional añade un nuevo éxito a la evolución de ambos sistemas de control de satélites.

GMV trabaja en la defensa planetaria de asteroides

PARA NUESTRA SOCIEDAD ES CRUCIAL EL CONOCIMIENTO Y COMPRENSIÓN DE LOS ASTEROIDES YA QUE AYUDARÍA A DETERMINAR EL PELIGRO REAL QUE SUPONDRÍAN PARA NUESTRO PLANETA (CADA VEZ MÁS DEPENDIENTE DE LAS COMUNICACIONES Y LA TECNOLOGÍA) EN CASO DE IMPACTO Y PONER REMEDIO A ESTE TIPO DE EVENTOS

En este contexto de defensa planetaria, es de gran importancia el desarrollo de las tecnologías, como las relacionadas con el Guiado, Navegación y Control (GNC) de sondas en proximidad de asteroides, que nos permitan realizar misiones para estudiar las características de los asteroides y de desviación por impacto en caso que fuese necesario.

GMV lleva años trabajando activamente en diversos proyectos en este campo. AIM (*Asteroid Impact Mission*), que dentro del programa AIDA (*Asteroid Impact and Deflection Assessment*) quiere estudiar los efectos del impacto de la sonda de la NASA DART contra la luna del asteroide Dydimos, demostrar nuevas tecnologías de comunicaciones ópticas en el espacio, así como caracterizar la superficie y estructura interna de Didymos y su luna; FCS ATOMIC (*Flight Control System Assessment Toolbox for Optimal Mission Cost and Performance*), iniciativa liderada por GMV con la que se pretende establecer un marco real de un Sistema de Control de Vuelo (*FCS-Flight Control System-*) conformado por los sistemas FDS y GNC, y sus respectivas interfaces, para valorar la viabilidad de futuras misiones. Y, TAIM (*Asteroid Impact Mission Thermal Infrared Imager*), nombre que recibe el estudio centrado en el desarrollo de una cámara termográfica que capta imágenes en el espectro infrarrojo para la misión AIM de la ESA.

Asimismo, durante este año GMV está participando activamente en el proyecto de defensa planetaria sobre asteroides de la Comisión Europea (CE), NEOShield-2. El proyecto, que arrancó en 2015 se enmarca dentro del programa I+D de la CE H2020,

Laboratorio Robótico Avanzado ***platform-art©*** de GMV

está liderado por Airbus Defense and Space GmbH, participan 11 empresas europeas y tiene un presupuesto total de 4.2 millones de euros.

NEOShield-2 desarrolla las tecnologías necesarias para las misiones espaciales con el fin de desviar asteroides amenazadores. El proyecto investiga además la forma de medir con precisión los intentos de desviación y cómo llevar a cabo investigaciones sobre el terreno. Se están analizando las observaciones astronómicas, la modelización, las simulaciones y la caracterización física de los objetos cercanos a la Tierra (NEOs, por sus siglas en inglés) para comprender mejor sus propiedades físicas. Por último, también intenta definir una estrategia europea para futuras actividades de investigación y asociadas a las misiones.

En el marco NEOShield-2, GMV se encarga del desarrollo del sistema autónomo de Guiado, Navegación y Control (GNC) basado en visión artificial, que permitirá aterrizar a la sonda en la superficie del asteroide, recolectar muestras de mínimo 30 gramos y retornarlas a la tierra; una misión clave para estudiar con precisión las características del asteroide antes de desviarlo. Asimismo, GMV desarrolla y opera bancos de pruebas para la validación en tierra de los tres sistemas GNC del consorcio NEOShield-2, para lo cual se está utilizando el laboratorio de Navegación Óptica y el Laboratorio Robótico Avanzado ***platform-art©*** , que permiten reproducir en tierra las condiciones del escenario espacial y estimular los sensores y ordenadores de abordo de la sonda espacial en tiempo real.

GMV presenta sus avances en materia de retirada activa de basura espacial

GMV ACUDE A LA *EUROPEAN CONFERENCE FOR AERONAUTICS AND SPACE SCIENCES*, EUCASS 2017, PARA PRESENTAR SU AVANCES EN MATERIA DE ADR

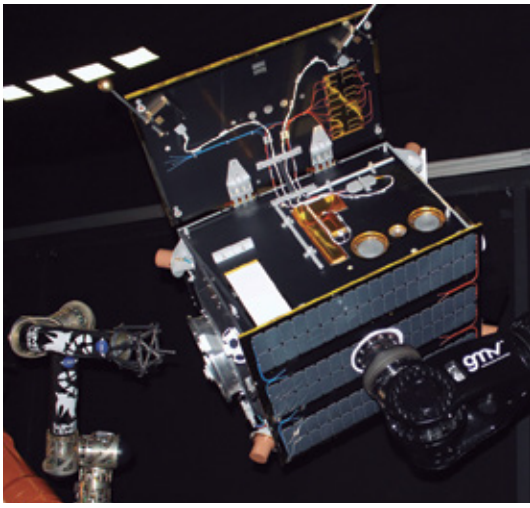
Del 3 al 7 de julio, GMV acudió a la séptima edición de la *European Conference for Aeronautics and Space Sciences*, EUCASS 2017, para presentar su avances en materia de ADR (Active Debris Removall), con la exposición de los resultados de tres proyectos que está desarrollando para la Agencia Espacial Europea.

El primero de ellos, SBSS-DM cuyo propósito es demostrar los objetivos de la misión SBSS (*Space-Based Space Surveillance*) enfocada en la vigilancia y monitorización tanto de objetos artificiales, así como cuerpos astronómicos (NEOs).

El segundo de los proyectos de investigación que se presentó fue AnDRoID, enmarcado dentro del programa IOD (*In Orbit Demonstration*), que focaliza en la captura de pequeños objetos de basura espacial (100-200kg).

Por último, el proyecto ORCO (*On Ground Validation of a Rigid Combo system*), que tiene por objeto consolidar, integrar y validar en tierra las tecnologías clave necesarias para llevar a cabo escenarios espaciales robóticos complejos (basados en "*Active Debris Removal for a small satellite*").

EUCASS, que se celebra desde 2005, es uno de los principales eventos científicos sobre aeronáutica y espacio del continente europeo, al que acuden científicos, investigadores y actores del mundo profesional no solo de Europa, sino también de Asia y América.



El proyecto ORCO tiene por objeto consolidar, integrar y validar en tierra las tecnologías clave necesarias para llevar a cabo escenarios espaciales robóticos complejos

GMV presenta el avance de los requisitos de observación para agricultura del programa Copernicus

GMV participó en la Jornada sobre Aplicaciones de Copernicus para el Sector Agrario, organizada por el Ministerio de Agricultura y Pesca, Alimentación y Medio Ambiente, en mayo en Sevilla, junto con la colaboración del CDTI y la Junta de Andalucía.

La Jornada, que es parte de la difusión Nacional del Programa Copernicus de la Comisión Europea, se centró en el impulso que supone la utilización de los datos de satélites del programa europeo Copernicus para monitorizar el estado del medio ambiente y la agricultura.

Julia Yagüe, Responsable de Servicios Copernicus de GMV, participó en la mesa redonda "Oportunidades para la Industria y Organismos Públicos de Investigación españoles"

En la actualidad, GMV lidera el contrato marco de la Comisión Europea que tiene como objetivo la definición de los requisitos de usuario de la futura generación de satélites del programa Copernicus mediante el cual Europa está dotándose de la capacidad y autonomía tecnológica para la Observación de la Tierra.

Hasta el momento la base de requisitos de usuario cuenta con casi 4.000 registros referidos a las 6 áreas de aplicación Copernicus como son vigilancia atmosférica, vigilancia ambiental marina, vigilancia terrestre, cambio climático, gestión de emergencias y seguridad.

Asimismo, GMV anunció el interés de la Comisión por extender el estudio de requisitos para el diseño del futuro componente espacio Copernicus a áreas transversales como la agricultura, recursos hídricos, patrimonio cultural, seguros o turismo.

GMV y Thales firman el contrato para el desarrollo de la nueva generación del CPFPS de EGNOS

Tras año y medio de negociaciones, GMV y Thales Alenia Space France firmaron, el pasado 16 de junio, un contrato de algo más de 10M€ para el desarrollo de la nueva generación de CPFPS (*Central Processing Facility-Processing Set*), también conocido como CPFPS-G2, contribución principal de GMV para la futura versión de EGNOS V2.4.2, que se espera sea certificada y declarada operacional a finales de 2019.

EGNOS (*European Geostationary Navigation Overlay Service*) es el sistema Europeo de aumentación (SBAS) de sistemas GNSS tradicionales como GPS y GLONASS. A lo largo de los años, GMV ha desempeñado un papel muy importante en este SBAS Europeo, trabajando en él desde sus fases iniciales en 1995. Desde entonces GMV ha participado entre otros en el desarrollo del CPFPS, elemento de software crítico y corazón del sistema que genera el mensaje con las correcciones que usará el usuario final, también en el desarrollo de otros elementos a nivel operacional como son el ASQF (Application Specific Qualification Facility), utilizado como soporte a la cualificación de las aplicaciones EGNOS; o en elementos de ingeniería como es el caso del EETES (*EGNOS End to End Simulator*), que se explota desde 1999 para generar los escenarios de referencia utilizados posteriormente durante las fases de validación, tanto de subsistemas como del sistema final.

El CPFPS que actualmente está desplegado y que proporciona las correcciones como parte del mensaje EGNOS, está funcionando gracias a una tecnología que data del año 1999, tanto en lo que se refiere al sistema operativo (RTOS) como a la parte de hardware. Dicha infraestructura ha quedado obsoleta hace ya varios años y actualmente se está volviendo cada vez más difícil de mantener. No obstante, GMV, a través del contrato actual de provisión de servicio de mantenimiento (CPFPS_PSS) asegura la viabilidad del mantenimiento del actual CPFPS en operación hasta 2021 sin problemas.

Equipo del Proyecto

Pero la realidad está ahí, y el problema de obsolescencia requiere el desarrollo de un nuevo CPFPS con nueva infraestructura hardware y software. Es por ello que se decide resolver el problema de obsolescencia para poder disponer de un nuevo sistema para finales de 2019.

Entre 2014 y 2015 GMV desarrolló la fase de diseño preliminar, donde se seleccionaron tanto el hardware como el sistema operativo para la nueva generación de CPFPS. Dicha selección se hizo siguiendo los requisitos de diversificación y homogenización marcados por la ESA.

A mediados de este año, concluidas las negociaciones donde se han refinado tanto el calendario como el alcance de las actividades a realizar, GMV y Thales Alenia Space–Francia han firmado el contrato para desarrollar la nueva generación de CPFPS y así asegurar la provisión de servicio de EGNOS V2 durante al menos otros 15 años más.

Pero esto no será todo, en un futuro a medio plazo, se tiene ya en mente implementar grandes mejoras algorítmicas así como la introducción de requisitos de misión, como por ejemplo la transmisión de correcciones para satélites GEO o "GEO ranging", aprovechando el hecho de tener un nuevo subsistema CPFPS con una infraestructura moderna y más eficiente.

GMV ha desempeñado un papel muy importante en este SBAS Europeo, trabajando en él desde sus fases iniciales en 1995

GMV encabeza el proyecto de la ESA para el control de la crisis migratoria a través de tecnología basada en satélites

De acuerdo con la Organización Internacional para las Migraciones (OIM), el número de personas migrantes y refugiadas que han llegado a Europa por mar se ha incrementado exponencialmente en los últimos años. Miles de personas han muertos tratando de encontrar mejores condiciones de vida.

En este contexto la Agencia Espacial Europea (ESA) ha adjudicado a GMV un estudio cuya finalidad es el desarrollo de servicios basados en técnicas espaciales y la utilización de macrodatos que ayuden en la identificación de los flujos migratorios humanos, estudiando su viabilidad técnica y proponiendo un plan para su aplicación y su aprovechamiento sostenible.

Con el respaldo de las principales partes implicadas en este ámbito y la colaboración de GMV Portugal, GMV UK encabeza este estudio de viabilidad que estudiará los requerimientos de entidades como la Organización Internacional para las Migraciones (OIM), Frontex, SatCen y EASO y, además, de otros agentes como ONG (*Conselho Português para os Refugiados*, AMI, Ayuda en Acción) y cuerpos nacionales de seguridad.

Este proyecto integra múltiples activos espaciales (Imágenes por Satélite, datos de GPS para geolocalización, comunicaciones por satélite, etc.); fuentes de macrodatos (Big Data), terrestres o derivados de activos espaciales (registros de datos de llamadas, datos de redes sociales, datos de observación de la Tierra, etc.) y se centra en tres fases identificadas de la gestión de emergencias (mitigación, preparación y respuesta).

Este estudio determinará el valor añadido de las soluciones basadas en macrodatos en el sector de la migración, es decir, la reducción de los riesgos de seguridad para migrantes, la mejora de los controles fronterizos y la prevención y respuesta a los problemas de seguridad relacionados con movimientos migratorios imprevistos. Asimismo, este estudio de viabilidad ayuda a conocer mejor a las personas que se desplazan y, de ese modo, a conseguir una mayor comprensión del fenómeno migratorio mejorando, al mismo tiempo, la eficiencia en la integración y la asistencia a las personas migrantes.

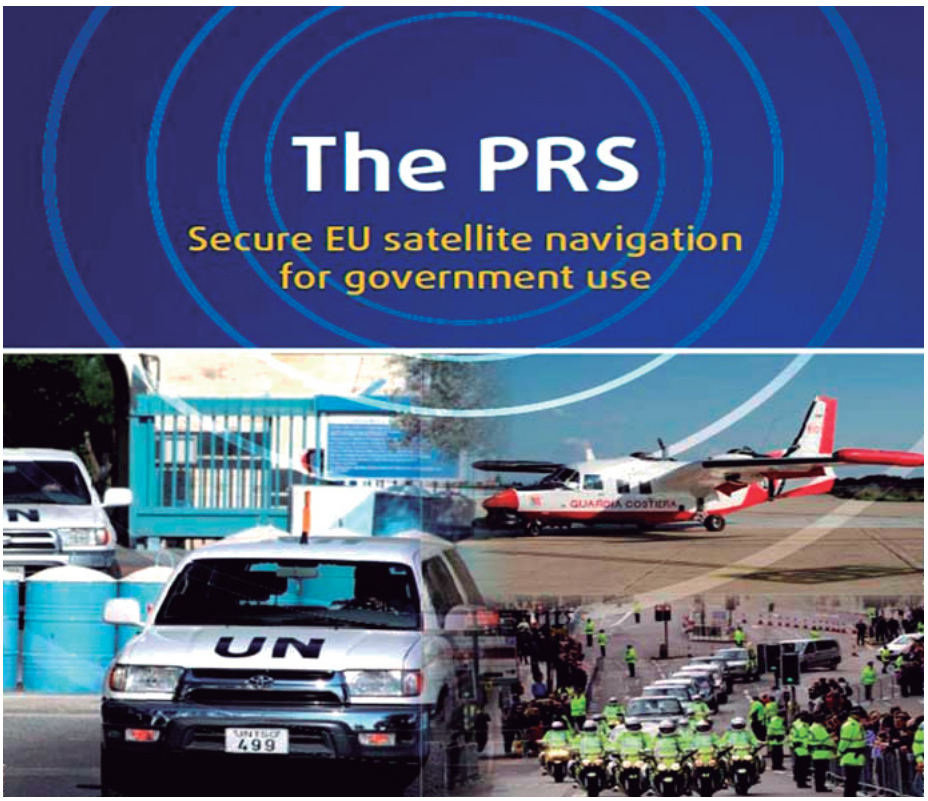
Una vez más, las tecnologías basadas en macrodatos tienen un papel fundamental que desempeñar en la obtención de información sobre migraciones y movimientos humanos aprovechando diversos activos espaciales (imágenes de observación de la Tierra, comunicaciones por satélite o sistemas globales de navegación por satélite (GNSS) e integrándolos en otros activos terrestres (datos de teléfonos móviles, de redes sociales, etc.).

GMV asiste al Encuentro con la ciencia y la tecnología de Portugal

GMV fue una de las empresas invitadas al encuentro Ciência'17, reunión anual de la comunidad portuguesa de ciencia y tecnología, que tiene como objetivo promover un debate abierto sobre los principales temas y retos que centran el trabajo de la comunidad científica portuguesa.

Teresa Ferreira, directora de Espacio de GMV Portugal, participó en la sesión "*Portugal Space 2030: Satellites, Antennas and Launchers*", en donde destacó la importancia de elevar el nivel de madurez tecnológica dentro de la industria nacional así como de reforzar y promover la cooperación internacional.

Ciência 2017 es un encuentro anual que recibe la ayuda del Ministerio de Ciencia, Tecnología y Enseñanzas Superiores y su organización está a cargo de la *Fundação para a Ciência e Tecnologia* en colaboración con Ciência Viva - Agência Nacional para a Cultura Científica y la Comisión Parlamentaria para la Educación y la Ciencia.



GMV abre camino para un mejor procesamiento de la señal PRS

LA AGENCIA ESPACIAL EUROPEA (ESA) HA VUELTO A CONFIAR EN GMV PORTUGAL PARA EL ESTUDIO DE TÉCNICAS DE PROCESAMIENTO PARA CIERTAS MODULACIONES DE LA SEÑAL GALILEO, COMO LAS UTILIZADAS POR LA SEÑAL DE SERVICIO PÚBLICO REGULADO (PRS)

En esta actividad, GMV, en colaboración con la Universidad Tampere de Finlandia y la Universitat Autònoma de Barcelona, ha sobrepasado los límites del estado de la técnica actual y mejorado sus resultados. Estos nuevos desarrollos serán de la máxima importancia en un futuro inmediato, dado que el rápido despliegue del Galileo y del nuevo servicio PRS requerirá una nueva categoría de receptores capaces de explotar todas las prestaciones de la señal. El PRS es un servicio de navegación encriptado para usuarios gubernamentales autorizados y aplicaciones sensibles que exigen una alta garantía de continuidad. De este trabajo se han redactado artículos que se han publicado en la IEEE *Signal Processing Magazine* y se han distribuido en la edición de este año de ION, una de las Conferencias GNSS de mayor prestigio.

Los conocimientos conseguidos se han materializado en el receptor de señal PRS de GMV, que se utilizará en escenarios operativos con el fin de demostrar el valor añadido de este servicio, además de consolidar la posición que ocupa GMV en el segmento de proveedores de receptores PRS.

GMV se incorpora a Eurospace.org como entidad asociada

CON UNA DEMOSTRADA POSICIÓN DE LIDERAZGO EN EL ÁMBITO ESPACIAL, GMV SE HA INCORPORADO RECIENTEMENTE A EUROSPACE, ASOCIACIÓN PROFESIONAL CREADA EN 1961 COMO ORGANIZACIÓN EUROPEA SIN ÁNIMO DE LUCRO CON EL OBJETIVO DE AGLUTINAR A LA INDUSTRIA ESPACIAL EUROPEA

Eurospace tiene como objetivos promover el desarrollo de actividades espaciales en Europa y ayudar a un mayor conocimiento de los problemas del sector. Reúne información relevante para el sector y mantiene un contacto permanente con la Agencia Espacial Europea (ESA), las Agencias Espaciales nacionales y, en general, con cualquier entidad que utilice o promueva la utilización de técnicas espaciales, como es el caso de los diferentes gobiernos europeos o la Unión Europea.

GMV se adhiere a Eurospace con el objetivo de contribuir con los conocimientos y experiencia adquiridos a lo largo de sus cerca de 35 años de actividad en el sector espacial y aunar esfuerzos para impulsar iniciativas que contribuyan al crecimiento de la industria espacial en Europa, generando empleo de valor al colaborar en el desarrollo de proyectos tecnológicamente avanzados.

Los miembros de Eurospace pertenecen a 14 países europeos distintos y, en conjunto, representan a más del 90% de la cifra de negocio total de la industria espacial europea, lo que hace de Eurospace la asociación con mayor representación del sector espacial en Europa.

Thales Alenia Space-Italia adquiere el sistema de planificación de misión de GMV para la segunda generación de satellites de COSMO-SkyMed

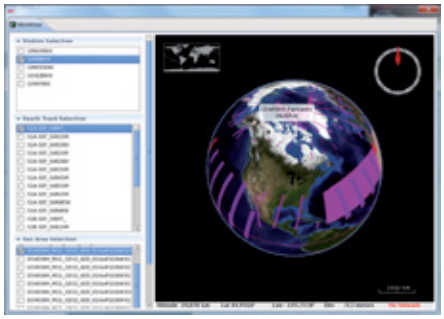
En 2016 Thales Alenia Space fue seleccionada por la Agencia Espacial Italiana (ASI) como Contratista principal para el desarrollo del programa COSMO-SkyMed (*COnstellation of small Satellites for the Mediterranean basin Observation*) Second Generation, que incluye una constelación compuesta de dos satélites con uso dual (militar y civil). Cada satélite está compuesto de un Radar de Apertura sintética (SAR) que es usado para la toma de imágenes de observación de la Tierra.

Recientemente, ***flexplan***, solución de GMV para sistemas de planificación de misión ha sido adquirido por Thales Alenia Space para ser evaluado como sistema de planificación de actividades de esta segunda generación de satélites de observación de la Tierra. ***flexplan*** utiliza un generador de algoritmos que permite implementar, cambiar y validar las reglas de misión y vuelo sin recompilarlas. Debido a esta flexibilidad, puede utilizarse para cualquier tipo de misión (órbita terrestre o interplanetaria), y se puede configurar, desplegar e integrar rápidamente en el segmento terrestre de una misión.

flexplan es un sistema operacional utilizado ya en misiones similares a este programa como son Sentinel-1, dentro del programa de la Comisión Europea Copernicus, compuesta por dos satélites, cuya carga de pago está también compuesta de instrumentación SAR; o el satélite PAZ, que forma parte del Programa Nacional de Observación de la Tierra (PNOTS) y del que se espera su lanzamiento y comienzo de operaciones para finales de este año.

Con esta adquisición, ***flexplan*** pasa a ser proveedor de una nueva Agencia Espacial Nacional que se suma a la ESA, la NASA, EUMETSAT y a la Agencia Espacial Coreana entre otras.

*Interfaz de usuario del Schedule Generation de **flexplan***



*Visualizador 3D del mapa del mundo de **flexplan***

La UK Space Conference reúne a la industria del sector

GMV, NO QUISO PERDERSE ESTA CITA BIENAL E ITINERANTE, QUE ESTE AÑO SE CELEBRÓ EN MANCHESTER DEL 30 DE MAYO AL 1 DE JUNIO

GMV asistió a la nueva edición de la UK Space Conference, donde mostró los productos y servicios que actualmente ofrece en el segmento espacio (sistemas de Guiado, Navegación y Control), en el segmento terreno (centros de control para satélites de telecomunicaciones, sistemas de procesado de datos de misiones de observación de la tierra, y aplicaciones usando datos y tecnologías espaciales) y en robótica.

Asimismo, GMV quiso hacer hincapié en las áreas que se desarrollan desde la filial británica y los proyectos que actualmente se están ejecutando en la misma, dentro del área de robótica. GMV participa el desarrollo de HRAF (*Harwell Robotics and Autonomy Facility*), así como en ERGO (*European Robotic Goal-Oriented autonomous controller*) dentro del marco europeo Peraspera. A su vez en observación de la Tierra, GMV desarrolla elementos de procesamiento para la misión de la ESA EarthCare, así como aplicaciones basadas en datos de satélite para soporte a la minería, la agricultura y a las crisis migratorias.

La UK Space Conference es uno de los mejores y mayores eventos en el sector espacial, tres jornadas de inmersión y networking, que ha logrado una vez más reunir a toda la industria del sector (gobierno, academia, clientes, proveedores, investigadores, etc) para compartir ideas, avances, desarrollos tecnológicos y novedades de la comunidad espacial, así como intercambiar visiones sobre cómo ese conocimiento puede operar cambios a nivel social, político y económico.

GMV aporta tecnología crítica para la misión Phobos Sample Return

GMV ENCABEZA EL CONSORCIO PARA EL DESARROLLO DE LA CÁMARA DE NAVEGACIÓN POR VISIÓN (VBNC, *VISION BASED NAVIGATION CAMERA*) DENTRO DE LA MISIÓN PHOBOS SAMPLE RETURN

El actual contrato de GMV con la Agencia Espacial Europea consiste en proveer de un modelo de ingeniería (EM, *Engineering Model*) de la aviónica de altas prestaciones para el procesamiento de las imágenes de navegación mediante algoritmos de extracción de características y búsqueda de correspondencias entre imágenes continuas de la superficie de Phobos, la luna más cercana a Marte.

La finalidad de la misión Phobos Sample Return (dentro de MREP -2) es regresar a la Tierra con muestras del suelo del satélite marciano Phobos, lo que supone un hito intermedio de cara al objetivo a largo plazo que es desarrollar las tecnologías críticas requeridas para la misión de Retorno de Muestras de Marte. GMV está desarrollando un sistema de Guiado, Navegación y Control (GNC) para la fase de aterrizaje el cual está basado en navegación autónoma mediante imágenes.

Además del modelo de ingeniería de procesamiento de imágenes, en el mismo proyecto se está desarrollando la unidad óptica de la cámara (COU) que consiste en las lentes, detector y aviónica de adquisición y pre-procesado de imágenes. La unidad óptica se integra con la tarjeta de procesamiento de imágenes para navegación (IPB) que a su vez conecta con un computador de vuelo el cual ejecuta los filtros de navegación del sistema de GNC. La selección de la aviónica de estos sistemas, y la implementación de los algoritmos de procesamiento de imágenes en dicha aviónica permitirá reducir los tiempos de ejecución desde el orden de decenas de segundos a centenas de milisegundos, lo cual es crítico para la rápida dinámica de descenso a tierra.

La finalidad de la misión Phobos Sample Return (dentro de MREP -2) es regresar a la Tierra con muestras del suelo del satélite marciano Phobos

En mayo tuvo lugar con éxito la revisión del diseño preliminar del proyecto, en el que GMV presentó el diseño de la arquitectura de la tarjeta de procesamiento de imágenes y los subsistemas de la unidad óptica de la cámara VBNC con la interconexión de todos los componentes. La arquitectura incluye componentes con capacidad para sobrevivir a las condiciones de la misión, centrado en el entorno marciano, y el diseño tolerante a fallos el cual incluye sistemas redundantes. Como validación de todo el sistema, GMV también presentó el equipo hardware de soporte en tierra en el cual se encuentra el computador de vuelo, para el cual se ha seleccionado el procesador Leon4 de 4 núcleos con RTEMS como sistema operativo de tiempo real.

Por último se presentó un plan preliminar de validación y verificación que abarca todo el proceso del ciclo de vida, desde las pruebas de las unidades hasta las pruebas del sistema a escala funcional, eléctrica y de entorno.

GMV invitada al seminario de Observación de la Tierra de la ESA

Las tecnologías de Observación de la Tierra (EO) se hallan en constante evolución, al igual que nuestra manera de procesar y explotar los datos de los satélites. Los beneficios científicos, sociales y económicos de estos datos son prácticamente infinitos, y es esencial aprovechar todo su potencial en estas tres áreas.

En este contexto, el día 11 de mayo, la Agencia Espacial Europea (ESA) organizó en ESRIN un seminario restringido en el que se abordaron los cambios de tendencia y las perspectivas en torno a este sector en los próximos años y al que asistieron representantes de todas las delegaciones nacionales, así como las principales empresas internacionales del sector, desde operadores y proveedores de satélites comerciales como Planet o SSTL, a proveedores de tecnología Cloud como Google Earth, Amazon Web Services, Microsofgot o Microsoft.

El acto, auspiciado por Josef Aschbacher, director de Programas de Observación de la Tierra de la ESA, abordó cuestiones tan actuales y abiertas como las constelaciones de micro satélites; las tecnologías de cloud computing, big data o Internet of Things; las políticas de datos abiertos a los datos o cómo conseguir que la sociedad se beneficie de forma generalizada de los datos de observación.

GMV, empresa de referencia en el área de observación de la Tierra fue invitada a participar en representación del sector tanto por la delegación portuguesa como por la delegación española representada por el CDTI. Al evento asistieron Luis Mariano González Casillas, director de la unidad de negocio de Procesamiento de Datos de Carga de Pago y Aplicaciones y Teresa G. Ferreira, Directora del área Espacial en Portugal.

Destaca el hecho que en España, GMV fue la única empresa participante gracias también a que GMV ha sido denominada por la Comisión Europea como Enlace Copernicus español.

GMV participa en la cumbre internacional "*Atlantic Interactions*"

Se constituirá un centro internacional de investigación para el Atlántico en las Azores a finales de 2018

La isla de Terceira, en las Azores, fue el lugar elegido para la celebración de la cumbre internacional "*Atlantic Interactions*", a la que asistieron representantes gubernamentales, empresas e instituciones académicas y científicas de 29 países, así como delegaciones de la Agencia Espacial Europea, la Comisión Europea, el Parlamento Europeo y las Naciones Unidas. En representación de GMV acudió el director general de Portugal, Alberto de Pedro Crespo.

El principal objetivo de la cumbre fue preparar la creación del Centro Internacional de Investigación (AIR Center) en las Azores, dirigido al estudio del Atlántico en áreas de espacio, cambio climático y la atmósfera, energías renovables y tratamiento de datos.

Como parte de esta cumbre, Manuel Heitor, ministro de Ciencias, Tecnología y Enseñanzas Superiores de Portugal, anunció la creación del Centro Internacional de Investigación para el Atlántico de las Azores a finales de 2018.

Se ha programado una nueva cumbre en noviembre, que tendrá lugar en Brasil y cuyo objetivo será revalidar los compromisos asumidos.

Arranca Urban GreenUp, proyecto H2020 para renaturalizar las ciudades

EL DÍA 7 DE JUNIO VALLADOLID ACOGIÓ EL ACTO DE PRESENTACIÓN DE URBAN GREENUP, PROYECTO FINANCIADO POR EL FONDO EUROPEO DE INNOVACIÓN E INVESTIGACIÓN HORIZONTE 2020 QUE TIENE COMO OBJETIVO DESARROLLAR UNA ESTRATEGIA PARA LA RENATURALIZACIÓN DE LAS CIUDADES A TRAVÉS DE SOLUCIONES BASADAS EN LA NATURALEZA

Acto de presentación del proyecto Urban Green Up

Aparte de los beneficios ambientales de este tipo de soluciones como incrementar la resiliencia frente al cambio climático y hacer las ciudades más saludables, el proyecto pretende también contribuir al desarrollo de la economía verde en el ámbito urbano, generando empleo y nuevas oportunidades y modelos de negocio. Además de acciones técnicas, incluye también actividades educativas, de participación pública y de concienciación ciudadana sobre los beneficios ambientales, económicos y sociales de las infraestructuras verdes.

Urban GreenUp, que está coordinado por la Fundación CARTIF y cuenta con la participación de un amplio consorcio internacional de 25 socios de 9 países de 3 continentes, tiene un presupuesto total de 14,81 millones de euros.

En España, el Ayuntamiento de Valladolid, a través de su Agencia de Innovación y Desarrollo Económico y con la colaboración de las Concejalías de Urbanismo y de Medio Ambiente, la Confederación Hidrográfica del Duero, los centros tecnológicos CENTA y LEITAT y las empresas Acciona, Singular Green y GMV, serán los encargados de llevar a cabo las actuaciones del proyecto previstas en la capital vallisoletana, que junto a Esmirna (Turquia) y Liverpool (Reino Unido) serán las tres ciudades demostradoras del proyecto.

En el contexto de este proyecto, GMV es responsable del paquete de trabajo relativo la monitorización de las medidas de renaturalización, cuyo propósito final es establecer un esquema de monitorización que permita evaluar el impacto de dichas medidas en la mejora de la capacidad de respuesta de las ciudades ante los retos mencionados (ej. el cambio climático). Este marco proporcionará un esquema de diagnosis y monitorización robusto basado en la evidencia de los datos.

Para ello GMV, junto a sus socios Urban GreenUP, ayudarán a las ciudades a definir e implementar una serie de indicadores de eficiencia clave (KPI, *key Performance Indicators*) y definirá una plataforma ICT compatible con las herramientas actuales y protocolos de trabajo de las ciudades. Los distintos socios del proyecto pondrán a disposición del mismo una serie de sensores in situ, aereotransportados y satelitales que, durante dos años, medirán los parámetros necesarios para calcular los indicadores de la eficiencia más adecuados para cada medida de renaturalización. Tras este periodo de monitorización, se realizará una evaluación global de los resultados en cada ciudad.

Asimismo, GMV desarrollará una aplicación para dispositivos móviles para fomentar comportamientos ecológicamente responsables en los ciudadanos. La aplicación móvil evaluará distintos aspectos del estilo de vida y las actividades de los usuarios (movilidad sostenible, ahorro energético, energías renovables, diseminación a terceros, etc) alineados con los KPI acordados, de modo que se le asignen puntuaciones en los distintos parámetros y una puntuación combinada. Para fomentar la participación de los ciudadanos, la aplicación permitirá organizar clasificaciones periódicas y eventos puntuales asociados a programas de incentivos.

El proyecto pretende contribuir al desarrollo de la economía verde en el ámbito urbano, generando empleo y nuevas oportunidades y modelos de negocio

GMV realiza una intensa campaña de pruebas con la plataforma robótica LUCID

LUCID (*LUNAR SCENARIO CONCEPT VALIDATION AND DEMONSTRATION*) ES UN PROYECTO DE LA AGENCIA EUROPEA DEL ESPACIO (ESA), LIDERADO POR GMV QUE TIENE COMO OBJETIVO DESARROLLAR Y EVALUAR LA COMBINACIÓN DE HERRAMIENTAS Y TÉCNICAS DE LOCALIZACIÓN Y PERCEPCIÓN DEL ENTORNO NECESARIAS PARA QUE UN VEHÍCULO DE EXPLORACIÓN PLANETARIA (ROVER) OPERE DE MANERA EFICIENTE Y SEGURA BAJO LAS LIMITACIONES AMBIENTALES Y OPERACIONALES DEL ENTORNO LUNAR POLAR

En el marco del proyecto, GMV ha integrado los equipos en el sistema y ha desarrollado el software de la plataforma robótica.

Durante este año la plataforma LUCID está siendo sometida a una intensa campaña de pruebas en Madrid y en Tenerife, en donde se está comprobando el correcto funcionamiento de todos los sistemas del prototipo del robot de exploración planetaria.

Fernando Gandía, jefe del proyecto LUCID, nos cuenta en qué consisten estas pruebas y cómo se están desarrollando.

¿Cuántos ensayos se realizarán dentro del proyecto?
Además de las dos semanas de pruebas preliminares en la Dehesa de Colmenar Viejo, se han programado otras cuatro semanas en Minas de San José, en el Parque Nacional del Teide, de las cuales ya se han completado las dos primeras. A lo largo del otoño volveremos a Tenerife para completar las dos restantes en las que realizaremos experimentos de más de dos horas de duración muy similares a la operación de una misión real.

¿En qué consisten?
El principal objetivo de las pruebas es evaluar diferentes combinaciones de técnicas de localización y de percepción del entorno (lo que en inglés se conoce como "*situational awareness*") que permitan a los equipos de operación de futuras misiones robóticas como LVP una percepción mucho más completa y fiable del entorno en el que se desplaza el rover. En este caso nos centramos en técnicas especialmente pensadas para los polos lunares que son áreas caracterizadas por condiciones de iluminación complicadas.

¿La elección de los lugares de estos ensayos responde a algún objetivo?
Aunque en nuestro planeta no es posible encontrar lugares que reproduzcan de manera absolutamente fidedigna todas las condiciones de los polos lunares, sí que existen determinadas regiones que pueden considerarse análogos lunares desde diferentes puntos de vista. En las Cañadas del Teide, en concreto, se dan ciertas similitudes en cuanto a la litología general del terreno y la estructura y composición del regolito (el material descompuesto que conforma el suelo que pisa el rover) que las convierten en un buen análogo del terreno que encontraríamos en el interior de los cráteres lunares. Además la isla de Tenerife es un destino muy conveniente desde el punto de vista de la logística.

¿Por qué son tan importantes la realización de diferentes pruebas dentro del proyecto?
Las pruebas son básicas por varios motivos. En primer lugar, son la mejor forma de validar de forma efectiva la interacción hombre/máquina, es decir de evaluar si la información suministrada por todas las técnicas en condiciones reales es suficiente para el operador y si la forma en que se le ofrece es la óptima. En segundo lugar son indispensables para conseguir aumentar la madurez y fiabilidad del sistema al enfrentarlo a condiciones de trabajo lo más reales posibles.

Aún pendientes de las últimas pruebas, ¿hay ya algunas conclusiones?
Aunque todavía es pronto para avanzar resultados, podemos decir que la primera parte de la campaña ha sido un éxito puesto que se ha conseguido ejecutar la totalidad del plan de pruebas previsto para las dos semanas de estancia en Tenerife. A lo largo de este tiempo conseguimos teleoperar el rover sin línea de vista del operador y en total oscuridad a través de terrenos complicados. Gracias a estas pruebas hemos obtenido información muy valiosa relativa a la utilidad concreta de cada una de las técnicas empleadas y a la forma en que el operador hace uso de ellas en función del terreno que atraviesa el rover. Durante la segunda parte de la campaña operaremos en condiciones de mayor dificultad (en trayectos más largos y con pasos más complicados). Además evaluaremos la utilidad de las mismas técnicas en el escenario de autonomía, en el que el rover es capaz de ejecutar planes complejos elaborados por un equipo de operación gracias a la información recibida del sistema.

Además del proyecto LUCID, GMV lidera otros proyectos de robótica espacial en el marco de la Comisión Europea (H2020): desarrollo del Sistema Operativo para el control de robots espaciales (proyecto ESROCOS); Sistema de Autonomía o inteligencia artificial (proyecto ERGO); coordinación de la Fase de Pruebas de los dos anteriores proyectos y otros más en diversos laboratorios europeos (proyecto FACILITATORS)

¿Veremos a LUCID en la LUNA en un futuro próximo?
FTR (el rover que empleamos en el proyecto LUCID) es un demostrador construido con equipos de uso terrestre y por lo tanto no está cualificado para viajar al espacio. Sin embargo, los equipos de diseño de misiones como LVP están esperando con gran interés los resultados de los análisis llevados a cabo en LUCID. Esta información les servirá para tomar decisiones de gran importancia relativas a la selección de los sensores y tecnologías que han de desarrollarse y montarse en los rover que viajarán a la Luna.

Equipo del proyecto LUCID en el Parque Nacional del Teide

Robdos Team camino a la ERL Emergency

Llevan trabajando desde el 2016 para crear su propio robot autónomo submarino. El objetivo es la competición ERL Emergency Robots 2017, un desafío multidisciplinar de robótica en el que, sobre un hipotético escenario de emergencia se compite de manera conjunta con un robot autónomo submarino, aéreo o terrestre, para evaluar el entorno, recopilar datos e identificar posibles peligros.

Robdos Team es el nombre del equipo que GMV apoya desde el 2016, con 13 integrantes que provienen de diferentes campos.

En 2016 se embarcaron en el proyecto de desarrollar su propio robot, WASABI (*Water-resistant Autonomous System for Assistance, Bathymetry and Inspection*), gracias a patrocinadores como GMV. Así empezaron con la construcción de un primer prototipo de plataforma, un catamarán de pruebas para poder trabajar simultáneamente, no solo en su construcción, sino también en la programación.

Las horas de trabajo han dado como resultado un robot autónomo modular, con el que ya trabajan desde principios del 2017 y que es capaz de adoptar distintas configuraciones en función de la actividad que vaya a realizar.

Actualmente Robdos team ultima los detalles para la European Robotic League (ERL) Emergency, evento que tendrá lugar en del 15 al 23 de septiembre de 2017, en Piombino, Italia, bajo la organización de la University of the West of England (Bristol).

Finaliza la ARGOS Challenge, la apuesta en I+D+i de TOTAL

TOTAL, el 4º proveedor de petróleo y gas a nivel mundial, ha organizado el "ARGOS Challenge" junto con la Agencia Nacional francesa de Investigación (ANR) con el objetivo de acercar el mundo de la robótica al sector industrial; demostrando su capacidad de innovación tecnológica. Las directrices de la competición eran diseñar, desarrollar y validar un robot autónomo de superficie, ideado para plataformas petrolíferas y de gas, capaz de llevar a cabo tareas de inspección y monitorización del entorno industrial, detectando anomalías e interviniendo en situaciones de emergencia.

Es la primera vez que se celebra esta competición y su desarrollo ha estado a la altura de sus participantes, 3 años de estimulantes desafíos en los que únicamente cinco formaciones han medido su ingenio a lo largo de tres rondas de desafíos.

GMV fue elegido de entre la treintena de equipos aspirantes, liderando el equipo FOXIRIS, del que también han formado parte IDMind (fabricante portugués de prototipos de robótico móvil) y UPM-CAR (el Centro de Automática y Robótica de la Universidad Politécnica de Madrid).

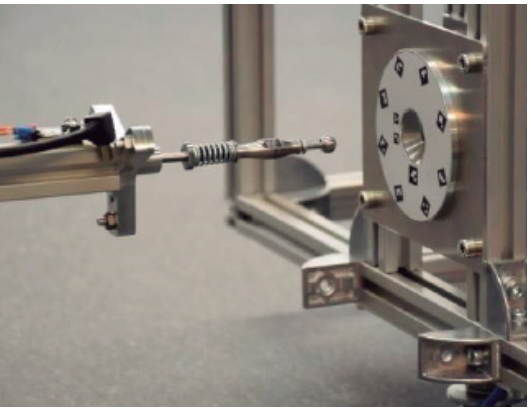
AIR-K (Japón), ARGONAUTS (Austria y Alemania), LIO (Suiza) y VIKINGS (Francia), fueron los equipos rivales de GMV durante esta competición que se desarrolló en Lacq, población al sur de Francia. Tras cada una de las rondas de competición (junio 2015, abril 2016 y marzo 2017), el Jurado Internacional era el encargado de emitir el informe técnico con recomendaciones para cada uno de los equipos y actualizar, asimismo, los criterios de evaluación para las pruebas de la siguiente competición.

Finalmente, el ARGOS Challenge se clausuró en la ceremonia de trofeos, el pasado 11 de mayo, en la torre Coupole de Total en París. Una vibrante noche donde se recogieron los hitos de estos tres años de competición y se hizo entrega de los trofeos, tanto al equipo ganador, los ARGONAUTS, como al resto de participantes, FOXIRIS, LIO, VIKINGS y AIR-K.

GMV fue elegido de entre la treintena de equipos aspirantes, liderando el equipo FOXIRIS, del que también han formado parte IDMind y UPM-CAR

Tecnología robótica para misiones de retirada de basura espacial y repostaje

EN MAYO TUVO LUGAR LA REUNIÓN DE ARRANQUE DE COMRADE (*CONTROL AND MANAGEMENT OF ROBOTICS ACTIVE DEBRIS REMOVAL*)



La finalidad del proyecto, de casi dos años de duración, consiste en diseñar, desarrollar y realizar pruebas con el sistema de control de un S/C robótico (incluido el manipulador y la mano robótica) para dos tipos de misiones: una de retirada activa de basura espacial (ADR) y otra de repostaje de objetos espaciales, que tendrán como referencias la misión ASSIST y la misión e.Deorbit respectivamente.

GMV encabeza el consorcio que llevará a cabo el proyecto y en el que participan también: ADS, que proporcionará los conocimientos necesarios sobre el nivel de sistemas de misiones espaciales, DLR, que aportará sus conocimientos casi únicos sobre robótica espacial; la Universidad de Burdeos, que se encargará de la implantación del control robusto; NTUA-CSL, que pondrá en juego su experiencia con ASSIST, lo que incluirá la configuración y prueba del escenario ASSIST en su banco de pruebas de cojinetes neumáticos; y por último PIAP, que pondrá su mecanismo de agarre a disposición del proyecto, diseñado para labores de ADR y más específicamente para la misión e.Deorbit.

Durante la reunión se fijaron los principales objetivos del proyecto y se aclararon los primeros pasos que se darán en el marco del mismo.

GMV afianza su posición en el mercado internacional de seguridad y defensa

GMV CONSIGUIÓ DURANTE EL EJERCICIO 2016 CIFRAS RÉCORD EN LA FACTURACIÓN INTERNACIONAL DE SUS ÁREAS DE SEGURIDAD Y DEFENSA, UN DATO SIN DUDA RELEVANTE TENIENDO EN CUENTA EL ENTORNO DE DIFICULTAD ECONÓMICA GLOBAL ASÍ COMO LA INCERTIDUMBRE PROVOCADA POR LA INESTABILIDAD PRESUPUESTARIA

Este hito supone la acreditación de GMV como referente internacional en ambas áreas, y se asienta principalmente sobre tres pilares: la contratación directa con agencias europeas, la venta de productos en el dominio JISR, por sus siglas en inglés (*Joint Intelligence Surveillance and Reconnaissance* -capacidad de Inteligencia, Vigilancia y Reconocimiento conjunta), y la participación en programas de I+D como el europeo Horizonte 2020.

GMV cuenta con una larga trayectoria de cooperación con agencias internacionales a través de contratos obtenidos mediante competición abierta. Colabora con la Agencia Europea de Defensa (EDA) desde su creación en 2004. En el marco del Programa de Inversión Conjunta de Protección de la Fuerza (*Joint Investment Program in Force Protection*) GMV fue la única compañía europea que consiguió ganar dos contratos. Esta estrecha colaboración con la EDA ha crecido en los últimos años y en la actualidad incluye relevantes áreas como la ciberdefensa, los sistemas C2 para el soldado a pie, o las arquitecturas de las Redes de Misión Federadas.

En el año 2010 GMV se convierte en el contratista principal para el diseño, desarrollo, mantenimiento, despliegue y evolución de la red Eurosur para la Agencia Frontex. La colaboración se inició con un proyecto piloto y en la actualidad la multinacional presta sus servicios a través de dos contratos marco con la citada agencia.

Por otro lado, para el Servicio Europeo de Acción Exterior (European External

Action Service) GMV es el contratista principal para el desarrollo y evolución del sistema de información de mando y control europeo (EUCCIS - *European Command and Control Information System*), utilizado por el EEAS en sus misiones en el exterior de Europa.

GMV también es colaboradora habitual de la Agencia Europea de Seguridad Marítima (EMSA) en actividades tales como estudios para identificar los beneficios para el usuario de sistemas aéreos no tripulados (RPAS) en el ámbito marítimo, o prestación de servicios TIC. En el ámbito de la teledetección y el procesamiento de imágenes de satélite, GMV colabora con SatCen (*European Union Satellite Centre*) a través de un contrato marco como contratista principal.

En el área JISR (*Joint, Intelligence, Surveillance and Reconnaissance*) y dentro de la participación española en el proyecto MAJIIC de la OTAN, GMV colabora tanto con diversas organizaciones de la NATO como con Ministerios de Defensa de países de la Alianza de ambos lados del Atlántico ofreciendo los sistemas SEISMO (Sistema de explotación de Inteligencia), CSD (*Coalition Shared Database*), Atenea (IRM&CM Tool) y COLLECTOR (*Simulador Sensores* ISR) que recopilan información de múltiples fuentes en diferentes formatos proporcionando a los analistas de inteligencia las herramientas necesarias para intercambiar información ISR y llevar a cabo flujos de trabajo que permiten la interacción en todas las fases del proceso JISR.

Asimismo, GMV tiene una destacada presencia en los programas marco de investigación en seguridad de la Comisión Europea, principalmente H2020 y su predecesor FP7. La actividad de la multinacional se ha centrado en el área de vigilancia marítima por medio de participación en diversos proyectos tales como CLOSEYE (*Collaborative evaLuation Of border Surveillance technologies in maritime Environment bY pre-operational validation of innovativE solutions*), EUCISE2020 y MARISA (*Maritime Integrated Surveillance Awareness*).

Estas actividades han consolidado la presencia internacional del área de Seguridad y Defensa de GMV, colocando a la compañía entre los principales actores del sector. Con base en los cimientos del impulso actual a la política europea común en Seguridad y Defensa, los planes de la compañía a medio plazo incluyen una consolidación de dicha presencia internacional asegurando un crecimiento sostenido.

Un paso más hacia el despliegue operacional de los sistemas SAPIIEM

COMO PARTE DE LAS ACTIVIDADES EN APOYO AL DESPLIEGUE DE LA CAPACIDAD JISR (*JOINT INTELLIGENCE, SURVEILLANCE AND RECONNAISSANCE*), GMV HA PROPORCIONADO APOYO A LA PARTICIPACIÓN DE LAS FUERZAS ARMADAS ESPAÑOLAS EN DIVERSOS EJERCICIOS EN EL ÁMBITO NACIONAL Y MULTINACIONAL

La ejecución de los procesos JISR se llevan a cabo mediante el empleo de los sistemas SAPIIEM (ATENEA, SEISMO, CSD, SIERRA Tools, C2NEC, COLLECTOR) desarrollados por GMV en el marco contractual con DGAM (Dirección General de Armamento y Material) del Ministerio de Defensa Español. Dichos sistemas han demostrado un alto nivel de interoperabilidad en ejercicios multinacionales, permitiendo intercambiar información con sistemas similares aportados por OTAN y otras Naciones.

Durante el primer semestre de 2017, las Fuerzas Armadas Españolas han hecho uso de estos sistemas en el ámbito de diversos ejercicios, entre los que destacan el ejercicio Nacional MOPEX, como ejercicio de evaluación del Mando de Operaciones (MOPS) en la planificación y dirección de una operación conjunta; el ejercicio OTAN STEADFAST COBALT 17 (SFCT17), en donde se prueba, evalúa y valida la interoperabilidad C4ISR para dar soporte a las Fuerzas NRF (NATO Response Forces) del periodo 2018, y en particular donde el Mando Conjunto de Operaciones Especiales (MCOE) se evalúa como Mando NRF18 de OTAN; y por último en el ejercicio SOCCEX de preparación nacional para el MCOE en vistas a la evaluación operativa OTAN que tendrá lugar a finales de año 2017.

El empleo de los sistemas SAPIIEM en todos estos ejercicios ha permitido llevar a cabo con éxito la ejecución de los procesos JISR, contando con el apoyo de GMV, considerándose un hito más hacia la implantación del despliegue operacional de estos sistemas.

El proyecto de Seguridad FORTRESS valorado por la Unión Europea como un éxito

Recientemente ha finalizado el proyecto FORTRESS (*Foresight Tools for Responding to cascading effects in a crisis*), proyecto de 3 años de duración financiado por la Comisión Europea, que ha tenido como objetivo conocer los efectos transfronterizos y en cascada de las situaciones de crisis en diferentes contextos de infraestructuras interconectadas.

El proyecto tenía como finalidad poder intervenir en prácticas de respuesta a crisis salvando la distancia entre una dependencia excesiva en la recogida no estructurada de información, por un lado, y una falta de atención a elementos de comunicación estructural y de gestión de situaciones de crisis transfronteriza y en cascada, por el otro. Para ello, ha utilizado las más avanzadas herramientas de recopilación de información y modelización para ayudar a todos los implicados a determinar qué información es significativa, relevante y de mayor prioridad, a fin de que puedan decidir en consecuencia cómo actuar.

Dentro del proyecto, llevado a cabo por trece socios de ocho países europeos, GMV ha encabezado el desarrollo de la Herramienta de Evolución de Incidentes (FIET), una herramienta de fácil utilización que calcula las infraestructuras, los sistemas y las áreas geográficas afectados por una emergencia incluso entre distintas organizaciones o países. La FIET puede utilizarse como herramienta de previsión y ayuda a la toma de decisiones, permitiendo a los responsables conocer de antemano los efectos potenciales de sus actuaciones en entornos de entrenamiento.

En definitiva han sido tres años de trabajo en el que se han logrado identificar efectos potenciales y generar conceptos innovadores, criterios de medición y estrategias para una mejor gestión intersectorial de las crisis. Unos resultados que han sido merecedores de una excelente valoración en la evaluación final de la Comisión Europea, cuyo veredicto ha sido que FORTRESS es un ejemplo de historia de éxito.

Primer despliegue en el marco del sistema de mando y control de la UE

ESTE HITO ES UN PRIMER PASO EN LA CONSECUCIÓN DE UN MARCO DE COOPERACIÓN A LARGO PLAZO COMO PROVEEDOR DE CONFIANZA DEL EEAS (*EUROPEAN EXTERNAL ACTION SERVICE*)

Dentro del contrato marco con el Servicio Europeo de Acción Exterior (EEAS) para el Mantenimiento, Soporte y Evolución del Sistema de Mando y Control de la Unión Europea (EU), en el que GMV actúa como contratista único, recientemente se ha realizado el despliegue en el entorno de producción del nuevo software que implementa las evoluciones requeridas durante el primer año de ejecución.

El Sistema de Mando y Control de la Unión Europea (EUCCIS) es el sistema utilizado por la EEAS en sus misiones en el exterior de Europa y permite planificar, monitorizar y conducir operaciones coordinadas por la EU para la gestión de crisis.

Las evoluciones implementadas en este primer año de ejecución se han centrado en conseguir una mayor adaptación del sistema a las necesidades de los usuarios y es de destacar el trabajo realizado en el portal colaborativo para el intercambio de información entre los puestos de mando desplegados en el teatro de operaciones y el centro de operaciones situado en Bruselas. En concreto, se ha rediseñado el portal para conseguir un cambio de paradigma que había sido solicitado por los usuarios con el objetivo de permitir una mayor adaptación del portal a las distintas comunidades de interés (en línea con esa colaboración entre distintos grupos tanto civiles como miltares) y una mejor segmentación de los contenidos relevantes para cada una de ellas.

Los nuevos componentes fueron desplegados en el entorno de producción en abril y las pruebas de aceptación (SAT, siglas en inglés de *Site Acceptance Tests*) fueron realizadas por los usuarios operativos durante mayo.

El Servicio Europeo de Acción Exterior (EEAS) ha manifestado su satisfacción por el trabajo realizado por GMV. El sistema ha podido ser desplegado y probado con éxito requiriendo muchos menos recursos y tiempo del que venía siendo habitual antes de la participación de GMV. Además, los usuarios finales han confirmado la mejora para su uso que proporciona el nuevo sistema. Finalmente, debe ser reseñado que el desarrollo realizado siguiendo un test-driven approach ha permitido que el número de incidencias detectadas durante todo el proceso de pruebas haya sido mínimo.

El sistema ha podido ser desplegado y probado con éxito requiriendo muchos menos recursos y tiempo del que venía siendo habitual antes de la participación de GMV

GMV en la última Conferencia de la OTAN en Portugal

El ciberespacio no tiene fronteras físicas y está expuesto a unas amenazas cibernéticas que están adquiriendo un poder disruptivo y destructivo cada vez mayor. A la vista de estos dos factores cruciales, la visión estratégica de la OTAN destacó la necesidad de establecer una capacidad cooperativa de ciberdefensa que pueda hacer frente a los retos actuales y futuros en los ámbitos de la seguridad y la defensa. Según el Concepto Estratégico de la OTAN, adoptado en noviembre de 2010 en Lisboa, el concepto de Defensa Inteligente trata de promover sinergias e impulsar los esfuerzos cooperativos de las Naciones Aliadas con el fin de garantizar el desarrollo la adquisición y el mantenimiento de las capacidades militares necesarias.

De ese modo, la Defensa Inteligente es asumida por la OTAN como forma de asegurar la no duplicación y la integración de iniciativas nacionales de desarrollo de capacidades (agrupar y compartir) en interés de una mejor priorización y coordinación de esfuerzos entre la OTAN y las Naciones Aliadas. En el área de la ciberdefensa, ya hay en marcha tres Proyectos de Defensa Inteligente: Multinational Cyber Defence Capability Development (MN CD2), Malware Information Sharing Platform (MISP) y Multinational Cyber Defence Education and Training (MNCDE&T). La Defensa Inteligente de la OTAN considera fundamental una cultura renovada de cooperación y requiere un enfoque innovador para la mejora de la ciberdefensa de la Alianza.

En la 3ª Conferencia de Ciberdefensa de la OTAN para Proyectos de Defensa Inteligente (CD SDP), celebrada en la Academia Militar de Amadora a finales de abril, se prestó especial atención a la cooperación entre la OTAN, el sector industrial y el mundo académico, así como a las nuevas oportunidades de colaboración entre la OTAN y la UE en el ámbito digital. En consonancia con esta idea, los Proyectos en el área de defensa de la OTAN (MNCD2, MISP y MNCDE&T) tienen como finalidad principal unir fuerzas y trabajar en común con empresas y centros de investigación y construir los puentes necesarios entre iniciativas nacionales e internacionales.

GMV, con experiencia demostrada en el sector de la Ciberseguridad, participó en la Conferencia para explicar de qué modo los últimos avances tecnológicos en Ciberseguridad y ciberdefensa pueden ayudar a resolver los retos a los que se enfrentan actualmente los diferentes cuerpos y fuerzas de seguridad estatales.

José Neves, director de Seguridad y Defensa de GMV Portugal, atendió a los representantes de los principales cuerpos y fuerzas de seguridad, que tuvieron oportunidad de visitar el stand de GMV y conocer de primera mano la estrategia de la compañía para este mercado.

GMV participa en la mejora de la vigilancia marítima europea

Common Information Sharing Environment (CISE) es una iniciativa promovida por la Comisión Europea para facilitar la vigilancia marítima en Europa que establece un proceso colaborativo entre autoridades para mejorar la conciencia situacional marítima.

Desde 2009, el concepto CISE está siendo desarrollado por la Comisión en colaboración con autoridades militares y civiles de los países miembro. Para ello se está definiendo un marco legal, político y organizativo para permitir el intercambio de información entre los sectores relevantes en el ámbito (defensa, fuerzas y cuerpos de seguridad del estado, salvamento marítimo, aduanas, fronteras, pesca y medio ambiente).

Como parte del trabajo de desarrollo de este concepto es necesario definir una serie de sistemas, redes y servicios que deben ser integrados en una infraestructura integral de información que permita alcanzar un CISE operativo para el año 2020.

Para ello, como parte del Séptimo Programa Marco, la Comisión ha asignado un proyecto de validación operativa denominado EUCISE2020. Este proyecto incluye 37 instituciones de 15 países incluyendo al Ministerio de Defensa a través de la Armada y otras instituciones españolas como Guardia Civil, Salvamento Marítimo y Agencia Tributaria.

Dentro de este proyecto se ha realizado una licitación de servicios de I+D a la industria para la creación de nodos EUCISE para intercambio de información. Estos nodos siguen una arquitectura basada en servicios definida usando NATO Architecture Framework (NAF) y empleando unos estándares técnicos para garantizar interoperabilidad entre nodos. En este proyecto GMV juega un papel clave gracias a su experiencia en interoperabilidad en entornos civiles y militares.

Esta aproximación tiene una clara coincidencia con la Arquitectura Global de Sistemas de Tecnologías de la Información y Comunicaciones del Ministerio de Defensa recogida en la Instrucción 58/2016, de 28 de octubre, del Secretario de Estado de Defensa.

Esta solución será desplegada en instituciones civiles y militares de varios países de la Unión Europea, en el caso de España se instalarán sendos nodos en Armada y Guardia Civil. Estos nodos serán validados en uso operativo durante un periodo de seis meses a partir de noviembre de 2017.

MARISA: Fusión de Datos y Big Data para el Tráfico Marítimo

En el Centro Regional de Vigilancia Marítima del Mediterráneo, un operador comienza su turno. Durante la guardia salta una alerta en su pantalla. Un buque mercante ha dejado de emitir AIS. El sistema indica que el buque sigue ahí porque fusionando los datos recibidos vía satélite, sabe que el barco mantiene la misma ruta que en las horas previas, la cual no se corresponde con la que debería seguir según la declaración de Puerto de Destino. El barco ha cambiado de bandera durante la travesía y suele hacerlo en esa época del año, pero cuando va a otro puerto. El software también detecta que entre la tripulación del mercante hay una actividad inusual en redes sociales, buscando enrolarse a otros buques, o haciéndose selfies para otras redes cuyos comentarios suenan a despedida. El historial del barco, sin embargo no muestra antecedentes de cargas no declaradas. Una vez evaluados todos los datos, el operador decide comunicar la alerta a su superior, que ordena una acción contra la actividad sospechosa del mercante.

Mientras tanto, otro operador, esta vez en el Mar del Norte, utiliza el software para evaluar las condiciones en las que se encuentra un buque de recreo al que le ha cogido por sorpresa una de las tantas y duras tormentas de ese mar. Es el momento de coordinar las actividades para un rescate.

Miembros del proyecto MARISA. Universidad de Laurea (Helsinki)

Estos escenarios podrán ser posibles en un futuro cercano gracias al proyecto MARISA (*Maritime Surveillance Awareness*) financiado por la Unión Europea como parte del Programa H2020 de I+D+i. En el Proyecto MARISA participan 22 entidades, entre empresas nacionales y multinacionales de cada país participante, instituciones de investigación nacionales y de la OTAN, y usuarios finales (Marinas militares, Guardias Costeras y la Guardia Civil española).

GMV, con un papel destacado en el proyecto, es responsable del diseño del sistema, del desarrollo de varios algoritmos de fusión y detección de anomalías, así como del iberian trial que se realizarán con la colaboración de la Guardia Civil y la Marinha Portuguesa.

En el marco del proyecto, iniciado oficialmente en mayo, la Innovación y el desarrollo en la frontera de la tecnología actual en lo relativo a Fusión de Datos Multisensor y Big Data son los motores principales, junto con la satisfacción de las necesidades operativas de los usuarios finales.

Jornada "Arquitectura global del Ministerio de Defensa, un modelo nacional de normalización e interoperabilidad"

En noviembre del año pasado se publicó la Instrucción 58/2016 de 28 de octubre, del Secretario de Estado de Defensa, aprobando la Arquitectura Global de Sistemas y Tecnologías de Información y Comunicaciones del Ministerio de Defensa. Esta arquitectura de referencia define una serie de principios para desarrollar sistemas para el Ministerio.

Con objeto de comunicar este hito, el día 29 de mayo el CESTIC (Centro de Sistemas y Tecnologías de la Información y las Comunicaciones) junto a la Fundación Círculo de Tecnologías para la Defensa y la Seguridad organizaron la "Jornada Arquitectura global del Ministerio de Defensa, un modelo nacional de normalización e interoperabilidad".

Inaugurada por Agustín Conde Bajén, secretario de Estado de Defensa, la Jornada incluyó una mesa redonda la que GMV intervino junto a otros respresentantes de las empresas del sector.

En esta mesa redonda Héctor Naranjo Setién resaltó "*que esta arquitectura resulta muy beneficiosa para empresas eficientes y con alta capacidad tecnológica como GMV ya que amplían las posibilidades de obtener licitaciones a partir de ofertas de alta calidad técnica gracias a la capacidad de aumentar la reutilización de componentes y tecnologías y a una más clara definición del trabajo a realizar*". "*GMV tiene una gran experiencia en el uso de todas estas metodologías, estándares y tecnologías que ha utilizado y está utilizando extensivamente en el marco de distintos proyectos tanto a nivel nacional como internacional*".

GMV en el escaparate europeo de Ciberseguridad

La Ciberseguridad está considerada a día de hoy como un asunto prioritario para la Comisión Europea. No sólo aparece como uno de los pilares de los programas marco de I+D de la UE, sino que ha pasado a la agenda de los políticos comunitarios y de los Estados miembros.

Lo cierto es que la Ciberseguridad es un factor crítico para garantizar la Transformación Digital de Europa, imprescindible para el avance tecnológico. Si no se logra desarrollar adecuadamente un sector fuerte con tecnología propia, estaremos expuestos a ciberataques cada vez más complejos y con mayor impacto en nuestra sociedad.

Con el objetivo de reunir a los expertos y compartir información sobre los últimos avances tecnológicos para combatir las amenazas a las que se enfrentan las organizaciones, se ha celebrado Infosecurity Europe 2017. Un evento considerado número uno en Europa y que ha colocado a Londres en el epicentro de la Ciberseguridad, marcado en la agenda por la profesionalidad de la audiencia procedente de todo el mundo y al que una empresa referente en el sector como GMV no podía faltar.

En el evento, los expertos de GMV han presentado la amplia gama de productos y servicios de Ciberseguridad, mostrando alguna de sus soluciones como ***gestvul***, ***checker ATM Security***, ***atalaya*** o ***arkano***. Además, han informado a los asistentes sobre otras soluciones como ***FARO Security***, una plataforma que supone un paso adelante en la mejora de la Gestión de la Seguridad actual en las organizaciones.

En resumen, un evento que contó con 240 ponentes, 360 expositores, unos 18.000 asistentes y en el que las soluciones de GMV estuvieron a la altura de las más avanzadas tecnologías existentes en el mercado de la Ciberseguridad.

GMV colabora con el CCI para abordar la Ciberseguridad Industrial

LA FORMA MÁS EFICIENTE DE PROTEGER LAS TECNOLOGÍAS DIGITALES DENTRO DE UNA PLANTA INDUSTRIAL ES RECONOCIENDO Y COMPROMETIÉNDOSE CON LA CIBERSEGURIDAD EN LAS PRIMERAS ETAPAS DEL CICLO DE VIDA

El entorno industrial está siendo afectado por las mismas vulnerabilidades y amenazas asociadas al entorno IT. Los expertos señalan que la forma más eficiente de proteger las tecnologías digitales dentro de una planta industrial es reconociendo y comprometiéndose con la Ciberseguridad en las primeras etapas del ciclo de vida. Esto significa incluir controles y medidas que cubran requisitos de ciberprotección para el correcto funcionamiento de un proceso industrial, y el proceso mismo, durante todas las etapas de producción (diseño, suministro, instalación y puesta en marcha).

El Centro de Ciberseguridad Industrial (CCI), con la participación especial de Técnicas Reunidas, ha publicado el documento "*Cybersecurity in an Industrial Automation Project Lifecycle*" que tiene como objetivo principal contribuir a la importante tarea de mejorar la protección de las infraestructuras industriales automatizadas. GMV ha contribuido aportando sus conocimientos y experiencia de la mano de Javier Zubieta, Responsable de Desarrollo de Negocio de Ciberseguridad de GMV Secure e-Solutions.

Con el creciente desarrollo de las tecnologías habilitadoras que dan forma al concepto de Industria 4.0, se abren cada vez más posibles vectores de ataque, que deben ser abordados con el fin de garantizar un funcionamiento seguro.

"Esta publicación permitirá cubrir la escasez de referencias normativas que tratan, de manera particular, la gestión de la Ciberseguridad en los sistemas de automatización y control industrial." **comenta Javier Zubieta**

La evolución hacia la inteligencia en la Ciberseguridad

"ES NECESARIO IR MÁS ALLÁ, APOSTAR POR UNA ESTRATEGIA PROACTIVA Y REACTIVA, ADELANTÁNDONOS A LAS AMENAZAS Y RESPONDIENDO ANTE ELLAS CUANDO SUCEDAN" JOSÉ MARÍA LEGIDO, DIRECTOR DE LA REGIÓN NORESTE DE GMV SECURE E-SOLUTIONS

A principios de año, IDC publicó una previsión en la que comentaba que más del 70% de las corporaciones iba a sufrir un ciberataque masivo antes de 2019, pocos meses después tuvimos el primer avance de lo que nos espera tras lo vivido en el mes de mayo con los ciberataques sufridos a nivel mundial de tipo ransomware infectando a miles de sistemas informáticos en decenas de países. En esta línea, José María Legido, Director de la Región Noreste de GMV Secure e-Solutions, nos desveló durante su intervención en la jornada de Predictions Barcelona, organizada por IDC e IDG, la importancia de disponer de un marco que permita gestionar los riesgos tecnológicos y de negocio, la arquitectura de seguridad, la concienciación del personal, la respuesta a amenazas y el cumplimiento legal (como es el caso del nuevo reglamento GDPR que entrará en vigor en 2018).

Legido destacó la falta de seguridad y las dificultades para identificar a los atacantes. "*Es necesario ir más allá, apostar por una estrategia proactiva y reactiva, adelantándonos a las amenazas y respondiendo ante ellas cuando sucedan*", comentó. Es fundamental ser conscientes del problema y el riesgo que supone esta amenaza en constante progreso que afecta a empresas, organismos públicos, servicios, personas, infraestructuras críticas y a nuevos paradigmas, como es el caso de la computación cuántica.

¿Podríamos llegar a ver las amenazas no conocidas? GMV propone el paso hacia la inteligencia del SIEM (Security Information and Event Management), convertir en inteligentes los ojos y oídos de nuestra plataforma IT. "*Existe la posibilidad de agregar eventos de los diferentes SIEM de la organización, añadir nuevas fuentes de información externas y/o internas y alimentar el SIEM con nuevas reglas inteligentes como el Big Data y Machine Learning*" añadió Legido. En concreto, se busca procesar y analizar grandes volúmenes de información, analizando casuísticas y comportamientos complejos con capacidades predictivas y analíticas avanzadas más allá de las posibilidades que ofrece un SIEM tradicional.

José María Legido considera que ante la nueva generación de amenazas que se avecina, la mejora de la seguridad requerirá de sistemas cada vez más inteligentes que sean capaces de detectar proactivamente las amenazas y actúen en consecuencia para prevenir o mitigar su impacto.

GMV refuerza su liderazgo en Ciberseguridad con Imperva

Imperva ha reconocido a GMV como Platinum Partner, siendo la primera empresa del Sur de Europa con esta categoría. Esta designación es la culminación de siete años de colaboración entre ambas organizaciones, ayudando a los clientes a implantar soluciones de Ciberseguridad para la protección de sus datos, así como a dar cumplimiento a la normativa vigente.

"*Este reconocimiento como Platinum Partner de Imperva nos distingue del resto, refuerza nuestro liderazgo en el ámbito de la Ciberseguridad y nos permite ofrecer a nuestros clientes las soluciones más innovadoras en la protección de datos y aplicaciones*", comenta Javier Zubieta, responsable de Desarrollo de Negocio de Ciberseguridad de GMV Secure e-Solutions.

Para conseguir la designación de Platinum Partner de Imperva, las empresas deben ofrecer una trayectoria demostrada de éxitos en la implantación y el soporte de la cartera de soluciones de Ciberseguridad de Imperva, integrada por las líneas de productos Imperva Camouflage, CounterBreach, Incapsula y SecureSphere. Deben reunir, además, muy amplios conocimientos y experiencia en el área de seguridad y dotar a su personal de recursos técnicos certificados por Imperva.

"*GMV es un socio comprometido y estamos realmente encantados de que se haya dado reconocimiento a su excelente labor y sus inversiones en Ciberseguridad*", explica Bertrand de Labrouhe, AVP para la región del sur de EMEA y Mediterráneo de Imperva. "*GMV e Imperva trabajarán juntos para ayudar a las empresas españolas a proteger los datos y aplicaciones críticos para su negocio, estén almacenados en sus propias instalaciones o en la nube. Además de ayudar a las empresas a prepararse para la entrada en vigor, después de mayo de 2018, del Nuevo Reglamento General de Protección de Datos (RGPD).*"

"GMV es un socio comprometido y estamos realmente encantados de que se haya dado reconocimiento a su excelente labor y sus inversiones en Ciberseguridad"
Bertrand de Labrouhe, Imperva

EAST FCS Forum, reúne a los expertos en protección de ATMs de todo el mundo

GMV HA PARTICIPADO COMO PATROCINADOR DEL EVENTO Y HA CONTADO CON LA ASISTENCIA DE PARTE DEL EQUIPO DE ***checker ATM Security***, EL PRIMER PRODUCTO DE SOFTWARE DISEÑADO ESPECÍFICAMENTE PARA PROTEGER LOS CAJEROS AUTOMÁTICOS CONTRA EL FRAUDE. CON 10 AÑOS DE EXISTENCIA ES A DÍA DE HOY LA SOLUCIÓN LÍDER PARA LA PROTECCIÓN DE ESTOS TERMINALES, CON MÁS DE 120.000 LICENCIAS INSTALADAS EN MÁS DE 40 ENTIDADES BANCARIAS

Los ataques lógicos a los cajeros automáticos están en aumento en Europa y en muchas otras partes del mundo. Un informe que cubre el año 2016, EAST (*European Association for Secure Transactions*) reveló que las ciberamenazas en este sector habían alcanzado su punto más alto en 2016. Los ciberdelincuentes se han servido hasta ahora del malware relacionado con el ATM, tarjetas de crédito clonadas y troyanos bancarios, sin embargo, los ataques se han diversificado en los últimos años. Con el fin de perpetrar estos ataques los criminales están buscando entrar en las redes de las instituciones financieras y luego iniciar un ataque desde el interior. En el otro lado del campo de batalla, los expertos en Ciberseguridad desarrollan soluciones para hacer frente a estas amenazas.

El EAST FCS Forum 2017 es un evento dirigido a los profesionales involucrados en la identificación, prevención y detección de riesgos de Ciberseguridad y delitos relacionados con cajeros automáticos. El evento se ha celebrado en La Haya (Holanda) y ha reunido a expertos de todo el mundo para compartir información sobre las últimas amenazas y contramedidas del sector financiero. Además, los asistentes han obtenido conocimientos prácticos sobre lo que las organizaciones están haciendo para combatir estos riesgos.

Self-Service Banking Asia 2017

GMV y Malaysian Electronic Payment System (MEPS) han compartido escenario para dar a conocer las nuevas amenazas de malware y las innovadoras soluciones que las empresas tecnológicas desarrollan y evolucionan constantemente. Esto ha tenido lugar en la "Self-Service Banking Asia 2017", congreso organizado por RBR (*Retail Banking Research*) y considerado evento de referencia sobre protección de redes de cajeros automáticos del Sudeste Asiático, una de las regiones de mayor crecimiento mundial en soluciones de Ciberseguridad en banca.

Carlos Sahuquillo, Cybersecurity Consultant de GMV, ha compartido sus conocimientos en la materia a través de la ponencia "*ATM Logical Security: adapting to new threats*", junto a Marcus Lim Wooi Loon, *Head Self-Service Terminal Business and Operations Division* en MEPS, dando a conocer cómo la asociación financiera asiática ha mejorado la ciberseguridad de su red de cajeros gracias a la colaboración con GMV.

El experto de GMV destacó durante su intervención la necesidad de adaptar los actuales modelos de Ciberseguridad que protegen las redes de cajeros: "*la situación reactiva actual debe de cambiar, vamos un paso por detrás, tenemos que pensar como un hacker y actuar de forma proactiva ante las amenazas*".

IDESCAT renueva el cumplimiento de las normativas ENS y LOPD

EL INSTITUTO DE ESTADÍSTICA DE CATALUÑA (IDESCAT) HA VUELTO A CONFIAR EN GMV LA ADECUACIÓN Y MEJORA DE SU ESTADO DE CUMPLIMIENTO RESPECTO A LAS NORMATIVAS DEL ESQUEMA NACIONAL DE SEGURIDAD Y LA LEY ORGÁNICA DE PROTECCIÓN DE DATOS

Para IDESCAT, GMV ha llevado a cabo una auditoría para identificar posibles no conformidades o aspectos susceptibles de ser mejorados. A su vez se ha trabajado en la mejora de aspectos organizativos para lograr el cumplimiento de ambas normativas y se ha llevado a cabo una revisión de las acciones puestas en marcha para incrementar la seguridad tras la auditoría que la compañía llevó a cabo en 2014.

En base a los resultados del examen realizado sobre todos los sistemas de información y ficheros (automatizados o no automatizados) del Instituto, así como sobre la seguridad física o la normativa de aplicación, GMV ha elaborado un plan de acción que se centra particularmente en las modificaciones que el ENS publicó el pasado 4 de noviembre de 2015.

Desde la primera auditoría, que GMV realizó a IDESCAT en 2011, la evolución en el cumplimiento de las normativas ENS y LOPD, así como en el estado de su seguridad, ha sido constante.

El ENS establece la política de seguridad en la utilización de medios electrónicos y está constituido por principios básicos y requisitos mínimos que permitan una protección adecuada de la información, creando las condiciones de confianza necesarias en el uso de los medios electrónicos por parte de los ciudadanos. Por su parte, la LOPD tiene por objeto garantizar y proteger lo que concierne al tratamiento de los datos personales, las libertades públicas y los derechos fundamentales de las personas físicas, y especialmente de su honor, intimidad y privacidad personal y familiar.

La innovación de GMV en los proyectos europeos de investigación sanitaria

LA INNOVACIÓN Y LA COLABORACIÓN PÚBLICO PRIVADA SON DOS DE LOS CAUCES POR LOS QUE DISCURRIR PARA LOGRAR EL OBJETIVO DE "VIVIR MÁS Y MEJOR" Y BENEFICIAR CON ELLO A LOS CIUDADANOS

Vivir más y mejor es una de las demandas de la sociedad y el objetivo con el que trabajan investigadores, médicos, ingenieros…. Profesionales de los sectores público y privado en el ámbito de la salud. La innovación y la colaboración público privada son dos de los cauces por los que discurrir para desembocar en él y beneficiar con ello a los ciudadanos. Todo ello, a través de una sanidad personalizada y centrada en el paciente, a la vez que sostenible en el tiempo.

Los Programas Europeos de Investigación persiguen también estos objetivos, financiando proyectos como FACET, HARMONY, MOPEAD o PAPHOS, en los que GMV participa aportando su alta tecnología. Estos proyectos requieren un gran esfuerzo de coordinación ya que implican a numerosos miembros de distintos países y diferente naturaleza.

En el caso concreto de Harmony, participan cincuenta y un socios europeos y GMV como única empresa tecnológica, investigando para mejorar y personalizar los tratamientos de pacientes con leucemia linfocítica crónica, linfoma no de Hodgkings, síndromes mielodisplásticos y bebés y niños con desórdenes sanguíneos. En este proyecto, GMV diseña y desarrolla una plataforma Big Data de análisis masivo de datos para ayudar a los médicos en la toma de decisiones.

En el proyecto MOPEAD para la investigación científica-clínica de la enfermedad de Alzheimer, GMV desarrolla una aplicación web basada en el concepto Citizen Science para el reclutamiento de pacientes con Alzheimer en fase temprana. A su vez, despliega e implanta un sistema Big Data para el análisis de los datos recogidos de estos pacientes.

En un escenario donde el cuidado preventivo y el bienestar cobran mayor importancia, y el tratamiento del diagnóstico y la gestión de enfermedades adquieren un grado de

certeza cada vez más elevado, a través del proyecto PAPHOS, GMV trabaja para crear una plataforma segura que, aplicando la nueva generación de tecnologías de analítica avanzada, permita a todos los actores involucrados en la atención sanitaria superar la fase de los informes (¿qué sucedió?), para alcanzar la predictiva (¿qué podría suceder?) y la prescriptiva (¿por qué sucederá?).

El hombre ha incrementado en treinta años su esperanza de vida y ahora el reto está en que los ganados sean de calidad. Para ello la UE ha impulsado el proyecto FACET, en el que GMV, a través de su plataforma de telemedicina ***antari HomeCare™***, pone al servicio de las personas mayores en estado de especial vulnerabilidad, cuyo riesgo de discapacidad puede llegar a ser elevado, una herramienta para cuidarlas, monitorizando y vigilando sus enfermedades crónicas, almacenando y gestionando sus datos de salud, así como planificando y haciendo seguimiento de sus terapias.

GMV participa aportando su alta tecnología en los proyectos FACET, HARMONY, MOPEAD o PAPHOS

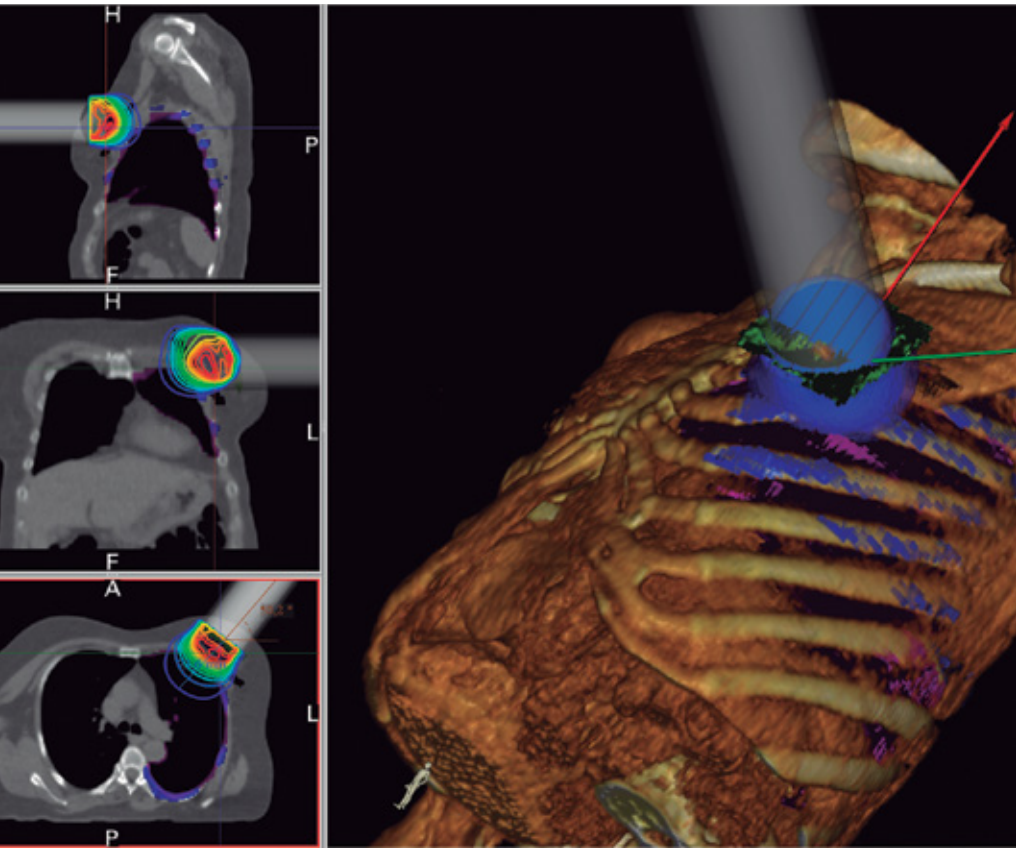
La tecnología de GMV al servicio del proyecto europeo RAINBOW

LA APORTACIÓN DE GMV PARA LOGRAR QUE LA MEDICINA PERSONALIZADA VAYA ALCANZANDO TODO SU POTENCIAL SE SUSTENTA EN SU AMPLIA EXPERIENCIA DESARROLLANDO SIMULADORES CLÍNICOS EXITOSOS COMO EL SIMULADOR QUIRÚRGICO ***insight*** O EL PLANIFICADOR DE RADIOTERAPIA INTRAOPERATORIA ***radiance***

GMV investiga en la concepción de la próxima generación de herramientas de simulación biomecánica que optimicen el diseño de tratamientos clínicos personalizados. Prácticas y fáciles de usar, los clínicos podrán manejarlas sin necesidad de la intervención de los técnicos. El trabajo que está desarrollando la compañía se enmarca dentro de RAINBOW, un proyecto incluido en la Innovative Training Networks (ITN) del programa Horizonte 2020.

El objetivo de RAINBOW "Simulación Rápida de Biomecánica para el Diseño Clínico Personalizado" es desarrollar conocimiento en áreas específicas de la simulación clínica. Para ello, se trabajará en tres vertientes: innovación e investigación, colaboración con la industria para medir el impacto clínico de los desarrollos y capacitación. El tiempo de duración de este proyecto son cuatro años en los que GMV colaborará con el resto de entidades participantes en la investigación, entre ellas, la Universidad Rey Juan Carlos, la Universidad de Cardiff de Gales; el Centro Nacional de Investigación Científica de Francia, la Universidad de Luxemburgo, el hospital Hvidovre y las Universidades Aalborg y Kobenhavns en Alemania, entre otros.

La aportación de GMV para lograr que la medicina personalizada vaya alcanzando todo su potencial se sustenta en su amplia experiencia desarrollando simuladores clínicos exitosos como el simulador quirúrgico ***insight*** o el planificador de radioterapia intraoperatoria ***radiance***.



BENEFICIOS DEL PROYECTO

Las habilidades de simulación, biomecánica, anatomía y fisiología que adquirirán los investigadores del proyecto RAINBOW serán de gran utilidad para desarrollar soluciones de diseño clínico computacional de próxima generación.

La apuesta de GMV por desarrollar tecnología de simulación de biomecánica rápida, de calidad de producción, así como por la formación de personal altamente cualificado en la materia, rubrica su compromiso con la innovación en las TICs sanitarias.

Tal y como ha confirmado Carlos Illana, Responsable de Producto en la firma, en el marco del proyecto RAINBOW y respondiendo al fin de la ITN "*se contribuirá a la formación de una nueva generación de investigadores creativos e innovadores capaces de transformar los conocimientos y las ideas en productos y servicios para el beneficio económico y social de la Unión Europea*". En este caso concreto, será en el desarrollo de herramientas de simulación clínica para ser aplicadas en el diagnóstico, pronóstico, seguimiento, entrenamiento quirúrgico, planificación, orientación, diseño de prótesis, operaciones de implantes y dispositivos médicos.

La plataforma e-Health de GMV da servicio a la Clínica colombiana Campbell y a la cadena de Ópticas 2000

La Clínica colombiana Grupo Campbell, institución líder especializada en el tratamiento de personas que han sufrido accidentes de tráfico, ha adquirido la plataforma de e-Health de GMV ***antari*** para el servicio de diagnóstico, prescripción y seguimiento de sus pacientes, agilizando de forma notable la gestión sanitaria en estas situaciones.

Asimismo, la versatilidad de esta plataforma, con desarrollos específicos para telepediatría y oftalmología, le ha permitido ampliar su presencia en una nueva cadena de ópticas líder como Ópticas 2000, empresa del grupo de distribución español, El Corte Inglés. De esta forma, la prestación de servicios de oftalmología en remoto, a través de ***antari***, se encuentra disponible en toda su red de establecimientos, a demanda de sus clientes.

antari, la suite de soluciones de eHealth y epidemiología de GMV, pretende dar respuesta y aportar un conjunto de soluciones a los retos actuales de la salud

Gracias a la plataforma de tele-oftalmología, desarrollada por GMV, que presta el servicio por videoconferencia en tiempo real, los clientes de las ópticas de la cadena de El Corte Inglés podrán disfrutar de un diagnóstico que, en muchas ocasiones, evitará la visita presencial al especialista. De esta manera, la firma añade valor al servicio que presta a sus clientes, ahorrándoles desplazamientos al especialista y otorgándole mayor confianza a la hora de adquirir sus gafas o lentes.

GMV comparte su experiencia de compra pública en salud

Carlos Royo, Director de Desarrollo de Negocio de Sanidad de GMV

La Junta de Castilla y León ha presentado su iniciativa de Compra Pública Innovadora para la modernización de los servicios de atención socio sanitaria a pacientes crónicos y personas en situación de dependencia de la región, en el evento "Colaboración empresarial en el sector TIC aplicadas a la salud y la alimentación", donde Carlos Royo, Director de Desarrollo de Negocio de Sanidad de GMV profundizó en la propuesta de GMV para contribuir a este objetivo.

Con la plataforma ***antari*** para la monitorización de pacientes crónicos pluripatológico, GMV se perfila como un sólido aliado capaz de contribuir a la implementación del proyecto impulsado por la Gerencia de Servicios Sociales, la Gerencia Regional de Salud y la Agencia de Innovación, Financiación e Internacionalización Empresarial de Castilla y León para facilitar el seguimiento de pacientes crónicos y personas en situación de dependencia.

El encuentro estuvo organizado por las Plataformas eVIA y Food For Life, con la colaboración de la Agencia de Innovación, Financiación e Internacionalización Empresarial de la Junta de Castilla y León y la Dirección Técnica de Ordenación y Acceso a los Servicios Sociales de la Gerencia de Servicios Sociales.

GMV incluye mejoras en el proyecto de modernización del transporte público de Chipre

El Departamento de Obras Públicas del Ministerio de Transporte, Comunicaciones y Obras de Chipre ha vuelto a confiar en GMV para el suministro de mejoras en el marco del proyecto de modernización tecnológica del transporte público de autobuses que actualmente se está implantando en todo el país.

Esta extensión incluye la instalación de 60 unidades de Videograbador a bordo, para el que GMV instalará la unidad embarcada REC30, que integra en un mismo dispositivo el equipo de localización, la gestión SAE y videograbador CCTV con difusión en tiempo real (*streaming online*) y que ya ha sido instalado y funcionando de manera exitosa en todos los autobuses de la isla de Malta, así con en otros proyectos desarrollados en España, Polonia o Malasia.

Aparte de a las cámaras IP a bordo, estos equipos se conectarán a TFTs para proporcionar información visual a bordo de los autobuses, así como a sensores de contaje de pasajeros a bordo.

El proyecto contempla el desarrollo de una página web de recarga electrónica de las tarjetas sin contacto que se van a poder usar a bordo de los vehículos de transporte público, y que utiliza la tecnología Desfire EV2. Para ello, GMV se tendrá que integrar con la plataforma de pago bancario JCC, que es la más extendida a lo largo de todo el país; una integración que puede suponer futuras extensiones con el objetivo de que la tarjeta que actualmente se usa en los autobuses pueda utilizarse más adelante en otros servicios gubernamentales.

Asimismo, el proyecto incluye la adaptación de una serie de vehículos para poder integrar el equipamiento embarcado que va a proporcionar GMV. Estos vehículos, principalmente furgonetas adaptadas para el transporte público, no cuentan con elementos clásicos de sujeción a bordo dado por lo que GMV ha tenido que llevar a cabo un replanteo completo de estos vehículos con objeto de encontrar soluciones personalizadas para cada modelo.

GMV presenta su gama de soluciones para transporte público en la UITP Summit

Del 15 al 17 de mayo GMV viajó hasta Montreal para asistir al 62º Encuentro Global sobre Transporte Público de la *International Association of Public Transport* (UITP).

La UITP es la organización internacional que reúne a todos los actores relevantes del sector del transporte público y funciona como red de contactos a nivel mundial para el intercambio de las mejores prácticas en esta área.

GMV presentó toda su gama de soluciones para transporte público, como sus sistemas de gestión de flotas para el transporte urbano e interurbano, sus sistemas de información de pasajeros y sus sistemas de ticketing. Asimismo, en el stand se presentaron demos de estas aplicaciones de ITS diseñadas para el transporte público.

Expertos de GMV en Tecnologías de Transporte Público también participaron en interesantes sesiones, en las que se incluyó la presentación de ***gmv planner*** powered by DPK, la última novedad de la cartera de productos de ITS, de GMV. ***gmv planner*** es una plataforma integral de Planificación y Programación que proporciona a las Autoridades de Transporte Público y Operadores una poderosa herramienta para gestionar todo el ciclo de vida de operaciones del Transporte Público.

El stand de GMV también dedicó un apartado exclusivo para su filial norteamericana, Syncromatics, en el que se presentaron demostraciones del sistema de gestión de flotas SaaS, personalizado para el mercado estadounidense.

Primera implantación de la solución óptima de planificación *gmv planner*

GMV HA SIDO CONTRATADA POR LA EMPRESA TRANSABUS DE TRANSPORTE COLECTIVO DE VIAJEROS DE MALLORCA PARA EL SUMINISTRO DE LA APLICACIÓN ***gmv planner***, HERRAMIENTA DESTINADA A LA PLANIFICACIÓN DE SERVICIOS EN LAS COMPAÑÍAS DE TRANSPORTE

El proyecto supone la primera referencia de GMV en España en este tipo de soluciones, que completan la actual oferta ITS de GMV, añadiendo una plataforma para la gestión del ciclo global del transporte, desde la configuración inicial de las líneas y horarios, pasando por la planificación de los servicios y el control de la operación, hasta los sistemas finales de información al pasajero.

gmv planner powered by DPK es una plataforma integral de Planificación y Programación que proporciona a las Autoridades de Transporte Público y Operadores una poderosa herramienta para gestionar todo el ciclo de vida de operaciones del Transporte Público. Resuelve de forma óptima la planificación de horarios y servicios y su distribución en calendarios de trabajo para vehículos y conductores, acorde a las reglas de negocio y restricciones existentes. Además, reduce los costes operativos e incrementa la oferta de servicios, recuperándose la inversión en un plazo muy corto y asimismo permite evitar tareas consumidoras de tiempo, trabajando rápida y eficientemente con una cantidad significativa de datos de forma integrada (solo el tiempo en planificación de calendarios de trabajo se reduce más de 20 veces).

Mediante ***gmv planner,*** Transabus pueden gestionar el ciclo de vida completo del servicio en un flujo de datos continuo a través de módulos integrados que soportan actividades que tienen lugar con distinto plazo y frecuencia:

- Planificación del servicio a largo plazo (vacaciones de conductores, red de transporte, horarios, servicios), medio (calendarios de trabajo de conductores y vehículos planificados), y corto plazo (correcciones de los nombramientos y cuadro horario).
- Soporte a la operación durante el servicio (despacho y control diario).
- Análisis a posteriori de la prestación efectiva de Servicio y su explotación en los sistemas corporativos (nóminas, ERP Corporativos / SAP, etc…)
- Planificación del mantenimiento en cada vehículo tras evaluar su servicio.

gmv planner ya ha sido implantada con éxito en operadores de transporte de carretera y ferroviarios, tanto europeos como asiáticos, siendo usada para gestionar la planificación del servicio de miles de vehículos

GMV introduce nuevas mejoras en el transporte de público de Szczecin

DENTRO DE LA LARGA RELACIÓN CON LA ZDITM SZCZECIN (AUTORIDAD DE TRANSPORTE DE SZCZECIN), GMV HA RESULTADO ADJUDICATARIA DE UN NUEVO CONTRATO PARA LA INCORPORACIÓN DE NUEVAS FUNCIONES AL SISTEMA DESPLEGADO EN 2015

ZDITM Szczecin es cliente de GMV desde 2010, año de la adjudicación y firma del contrato para la implantación de primera fase del Sistema de Ayuda a la Explotación (SAE), así como del sistema de información al usuario, del sistema CCTV en tiempo real y del sistema de emisión y validación de títulos de transporte. Desde entonces, las dos empresas no han dejado de colaborar para hacer aún más atractivo el sistema y el servicio de transporte público para los pasajeros.

En el marco de este nuevo contrato se han introducido mejoras en el sistema de información al viajero y en la herramienta de información del sistema de emisión y validación de títulos de transporte. Uno de los cambios más importantes para el cliente ha tenido lugar en el área de información al viajero, en el que una nueva función permite eliminar información estática de los paneles exteriores, así como de la página web en caso de que el vehículo no haya podido finalizar su recorrido por problemas técnicos. Gracias a esta función se podrá informar más rápidamente al viajero de todos los cambios que se produzcan en los servicios de transporte.

Además, las pantallas instaladas en los vehículos y los paneles de paradas y estaciones tendrán una nueva configuración, que permitirá a los viajeros saber si el vehículo que se aproxima ofrece la posibilidad de adquirir el billete en la máquina expendedora a bordo. Se mostrará información en pantalla cerca del destino, con pictogramas que indicarán las formas posibles de pago del billete en el vehículo (tarjetas bancarias, efectivo y monedero electrónico).

Estas nuevas funciones permitiran a ZDITM Szczecin adaptar el sistema a las actuales necesidades y proporcionar a los viajeros información de alta calidad para la planificación de su viaje

GMV incorpora nuevas funcionalidades al Sistema Inteligente de Transporte de Bydgoszcz

GMV ha firmado un contrato con la Autoridad de Transporte de Bydgoszcz, ZDMiKP, para renovar un año el servicio de mantenimiento de su Sistema Inteligente de Transporte (ITS en las siglas inglesas). Este nuevo contrato cubre el soporte técnico completo así como el mantenimiento de los equipos instalados en los 287 vehículos y los 35 paneles de información al viajero. GMV es también la encargada de suministrar una nueva infraestructura de servidores, desarrollar nuevas funcionalidades del sistema y adaptarlos para que den respuesta a las necesidades actuales del cliente.

Entre las nuevas funcionalidades destacan las modificaciones de la aplicación de gestión del contenido de los paneles instalados en la calle (Content Manager) y una aplicación para la creación y configuración de los datos topológicos para el ITS (Edition SAE). Asimismo, se realizarán cambios en los informes utilizados por la Autoridad de Transporte para las operaciones de liquidación con los operadores de transporte.

Una de las nuevas funcionalidades más importantes para el cliente es la aplicación "*Edition SAE*" para definir una versión de topología temporal. Esta modificación permite verter la topología actual temporal en una de las versiones de reserva y cargar una de las versiones de reserva en la topología temporal. Gracias a ello será posible trabajar con una topología histórica sin renunciar a la actual, copiando la topología actual en una de las topologías de reserva y después recuperando la histórica. Una vez finalizado el trabajo con la topología histórica, el usuario podrá cargar la topología anterior de nuevo en el sistema.

La cooperación entre GMV y la Autoridad de Transporte de Bydgoszcz comenzó en 2011, con la adjudicación y firma del contrato para la implantación del Sistema de Ayuda a la Explotación (SAE) con centro de control, para toda la flota de comunicación pública de Bydgoszcz. Desde entonces, GMV presta todos sus servicios a ZDMiKP con un alto nivel de satisfacción.

GMV refuerza su relación con Alstom

EL DÍA 4 DE MAYO TUVO LUGAR EN LAS OFICINAS CENTRALES DE ALSTOM, EN PARÍS, LA FIRMA DEL ACUERDO PARA LA INCORPORACIÓN DE GMV EN EL "*ALSTOM ALLIANCE CHARTER*", PROGRAMA MEDIANTE EL CUÁL ALSTOM PRETENDE REFORZAR SU COOPERACIÓN CON AQUELLAS EMPRESAS QUE CONSIDERA PROVEEDORES ESTRATÉGICOS

El objetivo de este programa es crear una red de alianzas prémium con proveedores clave dentro de la cadena de suministro de Alstom, que permita generar un marco de trabajo para conseguir objetivos comunes en torno a tres ejes principales: Desarrollo de negocio, Excelencia industrial y Producto e Innovación.

Este acuerdo, suscrito por Olivier Baril, *Chief Purchasing Officer* (CPO) de Alstom y por Miguel Ángel Martínez, Director General de Sistemas Inteligentes de Transporte en GMV, incluye objetivos específicos para ser desarrollados de forma conjunta entre ambas compañías, entre los que se incluyen el acceso a nuevos mercados y geografías, el desarrollo de funciones a medida para entornos de transporte multimodales, la identificación y desarrollo conjunto de nuevas funcionalidades para los sistemas AVLS (Automated Vehicle Location System) y el desarrollo de nuevas herramientas y sistemas relacionados con la eficiencia energética aplicada a los sistemas de transporte y movilidad.

Alstom y GMV llevan colaborando de forma activa desde 2014, año en el que ambas compañías firmaron un acuerdo marco para la homologación de GMV como proveedor de sistemas AVLS (SAE) para Alstom.

GMV acude a la nueva edición de la FIAA con nuevas innovaciones en Sistemas ITS

Un año más GMV acudió como expositor a esta nueva edición de la Feria Internacional del Autobús y del Autocar (FIAA), que tuvo lugar del 23 al 26 de mayo en Madrid.

Bajo el lema "Fabricando movilidad", la edición de este año se centró en soluciones innovadoras para el transporte por carretera dado que en próximos años estas tendrán una vital importancia en la reorganización concesional del sector. El evento reunió a autoridades, responsables políticos, distribuidores, fabricantes, instaladores, así como proveedores de soluciones asociadas al Transporte Colectivo de Viajeros por carretera.

Desde su stand GMV mostró sus sistemas tecnológicos de última generación, fruto de la búsqueda de soluciones innovadoras para satisfacer las necesidades de sus clientes en diferentes contextos (autobús, tranvías, BRT, etc.) y en diferentes ámbitos geográficos (Europa, Asia, África, América) en los que está presente la compañía, como son los productos ***gmv planner*** como herramienta de gestión óptima de los recursos de una empresa de transporte, el Sistema Ecodriving para control de la conducción y eficiencia energetica y los Terminales de Autoventa TVM en sus versiones embarcadas y compacta TVM-Mobile y de estacion TVM-Station.

GMV participa en el Plan de Movilidad Urbana Sostenible de Gijón

EL DESPLIEGUE DE UN SISTEMA MUNICIPAL DE CAR-SHARING ES UNA INICIATIVA DEL AYUNTAMIENTO DE GIJÓN EN EL MARCO DEL PLAN DE MOVILIDAD URBANA SOSTENIBLE, PARA MEJORAR LA EFICIENCIA DE LA FLOTA MUNICIPAL Y FOMENTAR LA MOVILIDAD LIMPIA Y SOSTENIBLE. CON ESTE PROYECTO, LA ADMINISTRACIÓN PÚBLICA Y LA EMPRESA PRIVADA UNEN SUS ESFUERZOS PARA MEJORAR LA CALIDAD DE VIDA DE LOS CIUDADANOS.

En el ámbito del proyecto, el Ayuntamiento ha remplazado su antigua flota de vehículos por un número menor de vehículos de uso compartido (48), de los cuales un 14% de ellos son eléctricos. Los vehículos de la flota de leasing han sido suministrados por Alphabet, actual cliente del servicio de gestión y localización de flotas de GMV, ***MOVILOC®***.

Como socio tecnológico, GMV se encarga del despliegue de una plataforma para la gestión de las reservas de los vehículos, que también permite gestión de viajes compartidos. El acceso a los vehículos se realiza a través de la tarjeta municipal de transporte, que controla el desbloqueo del vehículo y el arranque del motor. Los vehículos de la flota están equipados con el equipo móvil embarcado U10-D de GMV y un lector de tarjetas Mifare, y se integran la plataforma ***MOVILOC®***, para enriquecer el sistema con información adicional que permite la generación de informes y la monitorización de los vehículos en tiempo real.

En una segunda fase, el Ayuntamiento abrirá el servicio a ciertos colectivos de ciudadanos que se podrán beneficiar también de la flota municipal, mejorando así la intermodalidad del transporte público de la ciudad.

Moviloc destaca en la noche de transporte

El día 6 de abril, GMV se desplazó hasta Segovia para patrocinar la XVI ceremonia anual del Galardón Empresarial del Transporte, organizada por Asetra que este año cumple su cuadragésimo aniversario.

Un encuentro, con la Fundación Caja Segovia como escenario, en el que se destacó la labor de las empresas de transporte más relevantes del panorama castellanoleonés, por su aportación a esta comunidad.

Durante el evento, la Agrupación Segoviana de Empresarios de Transporte entregó el Acueducto de Plata a la Empresa de Transporte del Año a la compañía Transalbert. El valor añadido de esta empresa, especializada en el transporte frigorífico de mercancías perecederas y animales vivos a nivel nacional, ha sido la incorporación de ***MOVILOC®***, un servicio desarrollado por GMV para la gestión y localización de flotas.

El objetivo de Transalbert era conocer en tiempo real la temperatura de las mercancías transportadas, así como la hora de entrega de la mercancía. La implantación del sistema fue un éxito, así quedó patente con el galardón que recibió la empresa en 2015, en la V edición de los premios ITS, otorgados por la Asociación de Nuevas Tecnologías en el Transporte.

La solución tecnológica ***MOVILOC®*** lanzada en 2004, ha ido renovándose e integrando adelantos como el desarrollo del sistema para favorecer la ubicuidad del mismo, incorporando el servicio de acceso desde dispositivos portables (2015).

Entre otros reconocimientos, ***MOVILOC®*** recibió el máximo galardón en la categoría de ITS de los *Global Road Achievement Awards*, otorgado en 2006 por la Federación Internacional de Carreteras. Asimismo ha ganado concursos importantes a nivel internacional en Polonia, Malasia, Marruecos y Hungría.

GMV a la vanguardia de la movilidad sostenible

La celebración de la 22ª reunión de la Conferencia de las Partes en la Convención Marco de las Naciones Unidas sobre el Cambio Climático (COP22) en Marrakech a finales de 2016 resultó un hito más en la decidida apuesta estratégica del gobierno marroquí por liderar el desarrollo sostenible en África, tanto con fondos propios, como con apoyo de las organizaciones multilaterales.

En este contexto, GMV es desde hace años proveedor estratégico de sistemas tecnológicos para los principales operadores de transporte público del país africano, como son la multinacional local CityBus, la española ALSA o el operador ferroviario doméstico ONCF.

Recientemente CityBus ha vuelto a confiar en GMV el suministro de sistemas de gestión de flotas y billetaje al transporte público de Uchda. Con una población de aproximadamente medio millón, la ciudad rifeña es la octava ciudad del país y por su situación estratégica en la frontera, es el principal punto de paso con Argelia.

El sistema proporcionado por GMV en Uchda incluye el suministro de la moderna expendedora embarcada ETC-606, así como un módulo GPS/3G para el seguimiento y regulación en tiempo real de la operación. Además, este sistema permitirá a los usuarios, entre los que se encuentran numerosos estudiantes nacionales e internacionales, disfrutar del transporte público mediante el pago con tarjetas personalizadas.

Además, GMV opera desde hace años el sistema de geolocalización ferroviaria de ONCF con un moderno centro de control en Rabat. ONCF continua confiando en GMV, con la adjudicación de diversas ampliaciones entre las que cabe destacar la equipación de 95 trenes adicionales con el sistema embarcado diseñado por GMV, la implementación de una web para información a los pasajeros o el suministro de terminales móviles para alertas a operarios del sistema.

Con ambas adjudicaciones GMV renueva su indiscutible liderazgo en el mercado marroquí, donde actualmente está presente en el transporte urbano e interurbano de más de 10 ciudades.

Renfe confía a GMV la mejora del Sistema de Gestión de Flota de Renfe Mercancías

RENFE MERCANCÍAS HA VUELTO A CONFIAR EN GMV, ADJUDICÁNDOLE LA MEJORA DE SU SISTEMA DE GESTIÓN DE FLOTA, QUE RENFE DENOMINA INTERNAMENTE 'PLATAFORMA EMBARCADA DE COMUNICACIONES'

En 2007, GMV resultó adjudicataria de un primer sistema de gestión de flota para el área de Mercancías de Renfe. El sistema, que se termino de implantar en 2011, permitió equipar 387 trenes con la tecnología ***SAE-R*** de GMV.

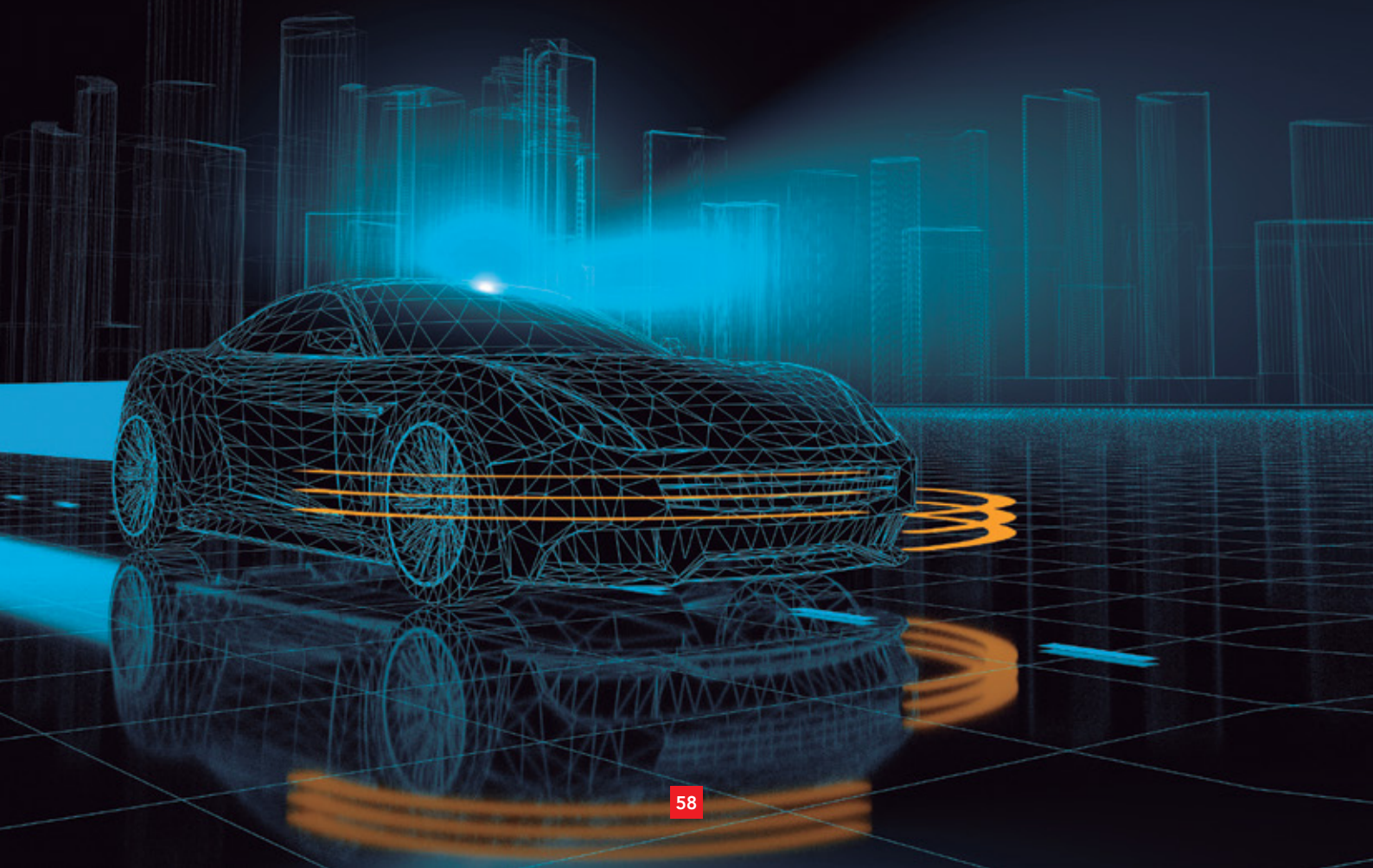
Con este nuevo contrato, con el que Renfe busca la mejora y actualización del sistema, se implantarán diversas mejoras, entre ellas la migración completa del Centro de Control actual a un entorno virtualizado en el CPD corporativo de Renfe, el cambio del sistema gestor de base de datos por el actual sistema que utiliza la compañía, así como otras mejoras gráficas que le dan un aspecto renovado y actual. Por último, se incorporan las últimas actualizaciones disponibles de la tecnología base del sistema ***SAE-R***, que lo adaptan a los nuevos sistemas operativos disponibles en el mercado para asegurar su mantenibilidad futura.

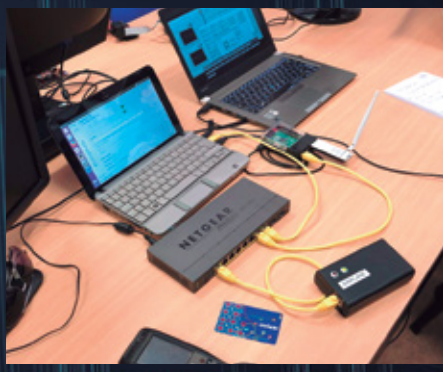
Este sistema completa el despliegue de la plataforma embarcada suministrada por GMV, que equipa a la totalidad de la flota de la operadora pública

Este sistema, junto con los ya suministrados para los trenes de Viajeros (Cercanías, Media-Distancia, Larga Distancia y AVE) completa el despliegue de la plataforma embarcada suministrada por GMV, que equipa a la totalidad de la flota de la operadora pública (más de 1.800 trenes y locomotoras).

Primeros resultados del proyecto ENABLE-S3 para la automatización y los sistemas de conducción autónoma

TRAS EL PRIMER AÑO DEL PROYECTO, A FINALES DE MAYO TUVO LUGAR LA REUNIÓN DE LA ASAMBLEA GENERAL DEL PROYECTO ENABLE-S3 (*EUROPEAN INITIATIVE TO ENABLE VALIDATION FOR HIGHLY AUTOMATED SAFE AND SECURE SYSTEMS*), EN LA QUE SE PRESENTARON LOS PRIMEROS DEMOSTRADORES, SIMULADORES Y VÍDEOS DE LO QUE SERÁN LAS PLATAFORMAS DEFINITIVAS DE ESTE PROYECTO QUE PREPARA EL CAMINO PARA LA AUTOMATIZACIÓN DE SISTEMAS CRÍTICOS





ENABLE-S3 es un proyecto de la Comisión Europea, que recibe financiación de ECSEL Joint Undertaking*, adjudicado a un consorcio de partners de más de 15 países y que tiene como objetivo preparar el camino para la rápida aplicación de sistemas de conducción con un alto nivel de automatización y sistemas de conducción autónoma en las esferas de la movilidad en carretera, aeroespacial, ferroviaria y marítima, así como en el ámbito de la salud.

GMV participa en dos casos de uso, lidera Traffic Jam Pilot with V2x, centrado en el área de automoción, y participa en Reconfigurable Video Processor for Space, liderado por Thales Alenia, con actividades centradas en el área de espacio.

En el caso de uso de automoción, las actividades de GMV darán lugar a un sistema piloto con un alto nivel de automatización que incrementará la seguridad del tráfico, reducirán la congestión y mejorarán los beneficios ambientales.

En el ámbito del Espacio, GMV aplicará las metodologías de ENABLE-S3 para validar un demostrador tecnológico bajo las extremas condiciones del espacio. Dicho demostrador será también resultado de este proyecto, y consistirá en el uso de FPGAs reconfigurables en vuelo para intercambiar implementaciones de navegación basada en visión según características de cada fase de una misión espacial.

Esto es, reutilizar el mismo hardware ahorrando costes y carga.
Los métodos virtuales de ensayo, verificación y selección de pruebas orientadas a cobertura que se llevarán a cabo en ENABLE-S3 permitirán reducir a un nivel razonable las actividades y costes de validación, dando lugar a una verificación y validación tempranas. El marco de validación resultante en este proyecto garantizará la competitividad para la industria europea en la carrera global de los sistemas de automatización.

La asamblea general del proyecto, celebrada tras el primer año después de su inicio, sirvió para seleccionar algunos de los desarrollos que se presentarán a la Comisión Europea.

Como participante en el proyecto, durante este encuentro GMV tomó parte en las diversas charlas en las que se discutieron las dificultades observadas durante el primer año de proyecto en los procesos colaborativos entre partners, así como para la definición de las actividades que necesitan ser abordadas dentro del mismo. Asimismo, GMV participó en las sesiones de trabajo (*break-out session*) correspondientes a sus casos de uso junto a sus partners.

Dentro del encuentro tuvo también lugar una jornada de exhibición de demostradores que permitió mostrar el trabajo e ideas, así como el estado de otros casos de uso.

* *ECSEL joint undertaking recibe soporte del programa de investigación e innovación HORIZON 2020 y Alemania, Austria, Dinamarca, España, Estados Unidos de América, Finlandia, República Checa, Italia, España, Portugal, Polonia, Irlanda, Bélgica, Francia, Países Bajos, Reino Unido, Eslovaquia y Noruega.*

GMV participa de manera activa en programas formativos sobre coche autónomo y conectado

LOS PASOS HACIA EL COCHE CONECTADO Y AUTÓNOMO SON CADA VEZ MÁS RÁPIDOS. MUCHOS HAN SIDO LOS AVANCES TECNOLÓGICOS Y LOS CAMBIOS QUE ESTÁN RECONFIGURANDO EL SECTOR, DE AHÍ QUE CADA VEZ MÁS SE NECESITEN PERFILES ORIENTADOS A ESTA DISCIPLINA. SI ESTO YA ES UNA REALIDAD, LOS AVANCES QUE SE ESPERAN PARA LOS PRÓXIMOS AÑOS HACEN NECESARIOS PROGRAMAS FORMATIVOS CONCRETOS PARA CUBRIR LAS NECESIDADES TÉCNICAS QUE REQUIERE UN SECTOR EN EL QUE GMV DOMINA DIVERSAS DISCIPLINAS RELACIONADAS

En el próximo año académico se inaugura la primera edición del Máster en Ingeniería de Vehículo Autónomo y Conectado, en el que GMV tendrá un papel activo, impartiendo sesiones a lo largo del mismo. Este programa formativo, desarrollado por la Universidad Politécnica de Madrid (UPM) y el Instituto Universitario de Investigación y Automóvil (INSIA), tratará sobre los aspectos relacionados con la ingeniería de los vehículos, su gestión en el sector y el impacto socioambiental que conllevan, entre otros temas. Su carta de presentación son los 25 años impartiendo el Máster en Ingeniería de Automoción y sus más de 20 años de experiencia en los Sistemas Inteligentes de Transporte.

GMV estará presente en el plan formativo y colaborará en materias relacionadas con la telemática, los sistemas ITS cooperativos y aplicaciones del vehículo conectado y autónomo. Se hará especial énfasis en casos prácticos en los que se han implementado las tecnologías en las que GMV tiene una amplia experiencia, como es el posicionamiento crítico de alta precisión y con integridad para vehículos autónomos, aspectos relacionados con la Ciberseguridad del vehículo autónomo y conectado, y soluciones tecnológicas concretas para aplicaciones en este tipo de vehículos.

En la misma línea formativa, el día 17 de junio concluyó la segunda edición del 'Curso de Especialización en Vehículo Autónomo y Conectado', organizado por ASEPA en colaboración con el Instituto Universitario de Investigación del Automóvil (INSIA-UPM).

Este curso, de un mes de duración y organizado en dos módulos (uno dedicado al Vehículo autónomo y otro dedicado al Vehículo conectado), contó con la participación de 16 expertos en estas especialidades, tanto investigadores y universitarios como representantes de las principales empresas y marcas más avanzadas en el campo de los vehículos autónomos y conectados. GMV colaboró impartiendo una de las sesiones, dedicada a presentar diferentes casos de aplicaciones de comunicaciones en el entorno vehículo, ofreciendo detalles sobre una amplia gama de servicios para vehículo conectado en los que GMV aporta una gran experiencia.

El Banco Interamericano de Desarrollo apuesta por la gestión del conocimiento

GMV ha trabajado con el Banco Interamericano de Desarrollo (BID) para implementar las bases de una infraestructura de gestión de conocimiento con el propósito de facilitar a los usuarios información que sea relevante, contextual y precisa. Para esto, GMV ha utilizado algunas de las tecnologías más adecuadas para el procesamiento de datos no estructurados, análisis cognitivo, Machine Learning y NLP (*Natural Language Processing*).

Gracias a su amplia experiencia y conocimiento técnico, el equipo de GMV ha logrado combinar y adaptar diferentes soluciones tales como IBM Watson y NLTK (*Python Natural Language Toolkit*) para dar respuesta a las necesidades específicas que requiere el BID en cuanto a gestión de conocimiento y procesamiento de información se refiere. Esto incluye la utilización de motores de análisis de conocimiento, algoritmos de extracción y organización de lecciones aprendidas de proyectos, así como clasificación automática de documentos.

Javier Fernández, responsable de la sección de Text Analytics & Big Data en GMV USA, ha liderado este proyecto que, según indica, ha permitido a GMV "*posicionarse como partner tecnológico líder en un área crítica en el BID como es la diseminación de conocimiento*".

El Banco Interamericano de Desarrollo es una de las principales fuentes de financiación a largo plazo para proyectos económicos, sociales e institucionales en América Latina y el Caribe. Además de préstamos, donaciones y garantías de crédito, el BID realiza proyectos de investigación de vanguardia para brindar soluciones innovadoras y sostenibles a los problemas más urgentes de esta región. Creado en 1959 para ayudar a acelerar el progreso en sus países miembros en vías de desarrollo, el BID trabaja día a día para mejorar vidas.

GMV ha utilizado algunas de las tecnologías más adecuadas para el procesamiento de datos no estructurados, análisis cognitivo, Machine Learning y NLP (*Natural Language Processing*)

RENLand distinguido con un premio Esri SAG

EL PROYECTO GIS DESARROLLADO POR GMV PARA REDES ENERGÉTICAS NACIONAIS (REN), EMPRESA PORTUGUESA CUYA PRINCIPAL ACTIVIDAD ES LA GESTIÓN DEL SISTEMA PÚBLICO NACIONAL DE DISTRIBUCIÓN DE ELECTRICIDAD, HA RECIBIDO RECIENTEMENTE UN PREMIO SAG (*SPECIAL ACHIEVEMENT IN GEOGRAPHIC INFORMATION SYSTEMS*), QUE RECONOCE EL PROYECTO MÁS IMPORTANTE, INNOVADOR Y DE MAYOR REPERCUSIÓN DEL AÑO

La principal misión de RENLand es controlar la vegetación que crece en la vía de paso del tendido eléctrico y las conducciones de gas y otras propiedades del Grupo REN, mediante la supervisión y el registro de actividades utilizando una solución de movilidad.

RENLand consiste en una solución colaborativa que da mayor agilidad y eficiencia al trabajo en equipo, facilitando la recopilación de información y el intercambio de información. Fruto de una larga alianza comercial entre GMV y ESRI, RENLAND se ha desarrollo utilizando la más avanzada tecnología de ESRI en el ámbito de los Sistemas de Información Geográfica (GIS). RENLAND es un concepto innovador con el que habían soñado los responsables de Propiedades y Derechos de Paso de REN, cuya finalidad es la gestión operativa y el mantenimiento de las vías de paso de tendidos eléctricos y conducciones de gas bajo la responsabilidad de REN.

La entrega del premio se realizó durante la Conferencia Esri User celebrada en San Diego, California, entre los días 10 y 14 de julio

GMV apoya el "IE Data Expedition 2017"

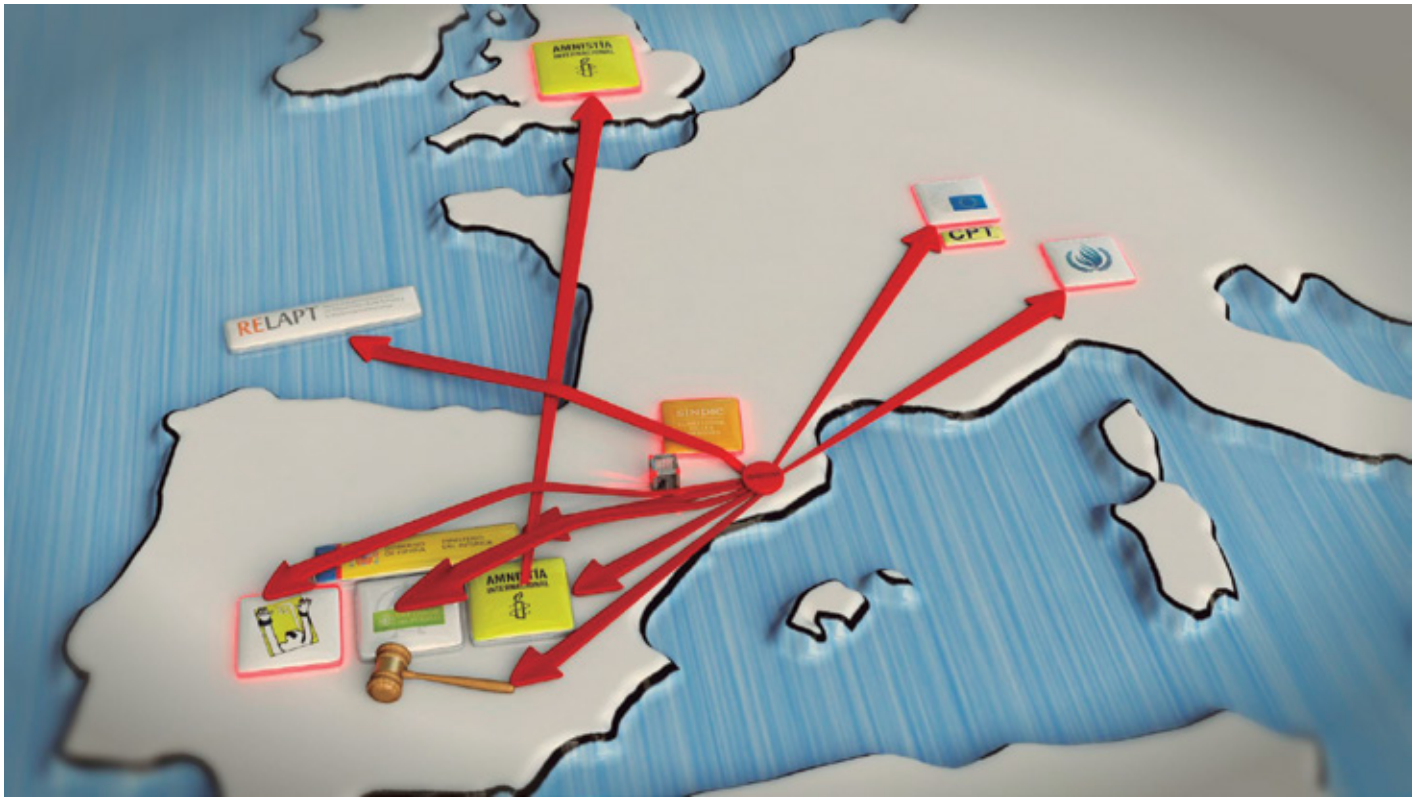
UN AÑO MÁS EL CLUB DE BIG DATA DEL INSTITUTO DE EMPRESA (IE) HA CELEBRADO EL "IE DATA EXPEDITION 2017", DATATHON QUE HA CONTADO DE NUEVO CON EL APOYO DE GMV COMO PATROCINADOR Y COLABORADOR EN LA ORGANIZACIÓN DEL EVENTO.

Durante dos días los participantes, en su mayoría estudiantes del Master en Big Data del IE, se enfrentaron al reto de resolver un caso real de negocio para el Banco Interamericano de Desarrollo (BID) a través del análisis de los datos proporcionados por la entidad bancaria. Este análisis nos mostraría como se difunde el conocimiento de expertos y el nivel de colaboración entre los distintos departamentos del BID. Los equipos podían elegir las herramientas que considerasen más adecuadas para completar las tareas, aunque desde la organización se les ánimo a utilizar modelos basados en grafos.

GMV fue invitada a colaborar por su gran experiencia en el ámbito del análisis de datos. Federico Sembolini, Data Scientist de GMV, participó como mentor y José Carlos Baquero, jefe de división y leader del grupo de Big Data de GMV, como miembro del jurado. GMV lidera iniciativas de Big Data y Business Analytics en áreas como la Ciberseguridad, la Prevención del Fraude, Sanidad, Industria 4.0 o la Agricultura de Precisión, entre otras.

El IE está reconocida como una de las principales escuelas de negocio del mundo, y ofrece un entorno internacional con estudiantes de todo el mundo y un alto nivel de formación. La competición ha contado con un nivel técnico muy alto, resultando una experiencia muy positiva y enriquecedora tanto para organizadores como para participantes.

Pionero sistema web en Europa para el Observatorio del Sistema Penal y los Derechos Humanos de la UB



EL OBSERVATORIO DEL SISTEMA PENAL Y LOS DERECHOS HUMANOS (OSPDH) DE LA UNIVERSIDAD DE BARCELONA (UB) HA PUESTO EN MARCHA EL SISTEMA DE REGISTRO Y COMUNICACIÓN DE LA VIOLENCIA INSTITUCIONAL (SIRECOVI) DESARROLLADO CON TECNOLOGÍA DE GMV

SIRECOVI es un sistema web pionero en Europa que permite a víctimas, informantes y organizaciones de defensa de los derechos humanos denunciar acciones de maltrato a través de un canal de comunicación privado. Casos de violencia institucional en cárceles, comisarías, centro de menores, centros de internamiento de extranjeros, así como determinadas actuaciones de las fuerzas de seguridad en la vía pública pueden ser denunciados de manera sencilla.

GMV ha desarrollado la plataforma garantizando la protección de los datos de carácter confidencial, con el fin de salvaguardar la privacidad de las personas

SIRECOVI permite a las organizaciones sociales y a la sociedad civil denunciar cualquier situación de presunta violencia institucional y activar los respectivos protocolos de protección de las víctimas. A su vez servirá para la investigación que se hace desde el Observatorio, permitiendo la creación de una base de datos para el estudio de la violencia institucional y la elaboración de un mapa donde se podrán visualizar todos estos casos.

SIRECOVI no sustituye en ningún caso los mecanismos procesales ni a la administración de justicia, sino que se erige como un mecanismo nuevo que el Observatorio proporciona para contribuir a evitar casos de violencia ejercida por parte de funcionarios del estado o de vigilantes privados que cumplan funciones de tipo público.

La puesta en marcha de este sistema cuenta con el apoyo del Ayuntamiento de Barcelona y ha sido posible gracias a un acuerdo entre el OSPDH y el Consell de l'Advocacia Catalana, que representa a los 14 Colegios de Abogados de Catalunya.

Industria 4.0 y Ecosistema de Innovación

EL FORO DE EMPRESAS INNOVADORAS HA ORGANIZADO EL EVENTO "INDUSTRIA 4.0 Y ECOSISTEMA DE INNOVACIÓN" PARA ABORDAR LA NECESIDAD DE TRANSFORMACIÓN Y MODERNIZACIÓN QUE REQUIERE EL TEJIDO INDUSTRIAL ESPAÑOL

El acto fue inaugurado por Juan M. Vázquez, Secretario General de Ciencia e Innovación del MINECO, Francisco Marín, Director General del CDTI y Luis Fernando Álvarez-Gascón, Director General de GMV Secure e-Solutions y Vicepresidente del FEI.

Durante el encuentro se ha hecho hincapié en la necesidad de transformación y modernización del tejido industrial, con particular énfasis en la conexión entre Industria y Ciencia. Para lograr este objetivo, los ponentes de las mesas redondas han resaltado la necesidad de realizar un diagnóstico de la situación actual y generar propuestas políticas de innovación, a través de un debate con los actores relevantes y representativos del ecosistema en torno a la Industria.

Luis Fernando Álvarez-Gascón se refirió a la velocidad de los cambios como característica del proceso de transformación de la Industria 4.0. En este sentido, manifestó que España debe esforzarse por mantener un ritmo evolutivo elevado que le permita alcanzar el nivel de bienestar social 4.0. La aspiración de llegar al máximo nivel de bienestar social requiere de una reinvención por parte del sector industrial español, asumiendo la necesidad de abordar un proceso de reindustrialización que implique una mayor aportación al PIB por parte del sector, mediante un desarrollo que no debe limitarse a las empresas del ámbito tecnológico, sino que debe llevar la revolución 4.0, incluso hasta el sector primario.

Asimismo, el Vicepresidente del FEI y Director General de GMV Secure e-Solutions expresó la necesidad de que nuestro país incremente su inversión en I+D+i, mediante mayores aportaciones tanto públicas como privadas. A ello, aseguró, "*debe acompañarle un debate sobre las políticas e instrumentos más adecuados de cara a optimizar el resultado de las inversiones que está realizando España*".

Por su parte, Juan M. Vázquez, Secretario General de Ciencia e Innovación del Ministerio de Economía, Industria y Competitividad, expresó su convicción de que una mayor dotación presupuestaria con destino I+D+i y un aumento de la inversión por parte de las empresas, se reflejarán en un incremento del peso del sector industrial en el PIB.

TECHFEST: Fomentando la tecnología y la gestión de datos

Cada vez más, los datos son una fuente de información muy valiosa y codiciada en el mundo empresarial. Son muchos los profesionales que dedican mucho tiempo a su investigación y análisis para extraer información de interés, ayudando en la toma de decisiones y provocando grandes beneficios a compañías e instituciones.

La Escuela Técnica Superior de Ingeniería Informática de la Universitat Politècnica de València (ETSINF-UPV) ha celebrado del 2 al 4 de mayo el TechFest 2017. Un evento que ha reunido a grandes profesionales del ámbito del Big Data para presentar la evolución y los avances de esta tendencia.

Carlos Sahuquillo, Consultor de Ciberseguridad de GMV, miembro de ISACA Valencia y de la Cloud Security Alliance, ha sido uno de los expertos en participar en estas conferencias. A través de la ponencia bajo el título "*¿Qué uso hacen las empresas de nuestros datos?*", Carlos ha explicado a los asistentes qué tipo de información guardan las grandes empresas de cada uno de nosotros y con qué fin (algunas simplemente por mejorar su servicio, otras con fines publicitarios y otras por ganar dinero con ellos). "*En un futuro tendremos medicina proactiva gracias a los datos que nuestros dispositivos de monitorización, pulseras de actividad y relojes inteligentes recogen de nuestro día a día*" comentó Sahuquillo.

El evento ha centrado su objetivo en el fomento de la tecnología y la gestión de datos en las próximas generaciones de profesionales de los ámbitos de la informática, la robótica y la electrónica. Ponencias, charlas, talleres y concursos en torno a la gestión de datos abiertos y las tecnologías han compuesto las actividades del programa del TechFest, un evento organizado por la Cátedra de Transparencia y Gestión de Datos.

Arranca el proyecto PRODUCTIO del CDTI, liderado por GMV

GMV LIDERA EL CONSORCIO QUE SE CENTRA EN INVESTIGAR SOBRE NUEVAS TECNOLOGÍAS QUE MEJOREN LOS PROCESOS DE MANTENIMIENTO INDUSTRIAL, QUE AYUDEN A PREDECIR LAS ANOMALÍAS Y FALLOS, REDUCIENDO LOS TIEMPOS DE PARADA Y AUMENTANDO LA DISPONIBILIDAD DE LAS MÁQUINAS

PRODUCTIO (*PROductivity InDUstrial EnhanCement through enabling TechnlOgies*) es un proyecto en el que participan un Consorcio Nacional de I+D multisectorial y multidisciplinar, con el objetivo de "*investigar sobre diversas tecnologías, técnicas, herramientas, metodologías y conocimientos dirigidos a aumentar la capacidad operativa de los procesos industriales (Overall Equipment Efficiency – OEE) en el marco de la industria conectada*", según palabras de Miguel Hormigo, responsable de los proyectos de Industria 4.0 de GMV. El proyecto permitirá la adopción de soluciones productivas y de mantenimiento en la industria conectada y facilitará la confianza digital mediante nuevos enfoques de seguridad.

Recientemente se ha celebrado la reunión de arranque, inaugurada por Luis Fernando Álvarez-Gascón, Director General de GMV Secure e- Solutions, conducida por Miguel Hormigo, Director de la Región Sur de GMV Secure e-Solutions y con la presencia de los directores generales y directores de innovación de las empresas participantes: Gonvarri, Fagor Arrasate, Hiperbaric, Zener, Industria PuigJaner, Tecnomatrix y de algunas de las entidades y compañías colaboradoras como Instituto Tecnológico de Castilla y León, Tecnalia, Eurecat e Ikerlan.

GMV lidera dicho Consorcio que se centra en investigar sobre nuevas tecnologías que mejoren los procesos de mantenimiento industrial, que ayuden a predecir las anomalías y fallos, reduciendo los tiempos de parada y aumentando la disponibilidad de las máquinas. Tecnologías como técnicas de inteligencia artificial en mantenimiento predictivo de las instalaciones de línea blanking; mantenimiento predictivo y asistido para poder monitorizar y mantener máquinas distribuidas por el mundo; tecnologías novedosas de fabricación relacionadas con la industria conectada que apoyen a la toma de decisiones en la fase de producción y mantenimiento; predicción de fallos en sistemas y fórmulas para mejorar el nivel de eficiencia global del proceso industrial utilizando herramientas analíticas Big Data; en definitiva, obtener conocimiento para convertir máquinas/herramientas en sistemas ciberfísicos que permitan mejorar aspectos de fiabilidad, rendimiento, disponibilidad, productividad y calidad; y en tecnologías que permitan asegurar la integridad de los datos de sensores y evitar el uso fraudulento por parte de los usuarios.

Según destacó Miguel Hormigo, "*este proyecto aunará los objetivos particulares de las empresas y entidades participantes alrededor de interés común: incrementar la productividad y la competitividad de nuestra industria, a la vez que convertir el proyecto en un referente de Industria 4.0*".

GMV participa en dos de los dieciséis proyectos que ha aprobado el CDTI (Centro para el Desarrollo Tecnológico Industrial), en su convocatoria de 2016, del Programa Estratégico de Consorcios de Investigación Empresarial Nacional (CIEN) que financia grandes proyectos de investigación industrial y de desarrollo experimental, desarrollados en colaboración efectiva por agrupaciones.

El proyecto permitirá la adopción de soluciones productivas y facilitará la confianza digital mediante nuevos enfoques de seguridad

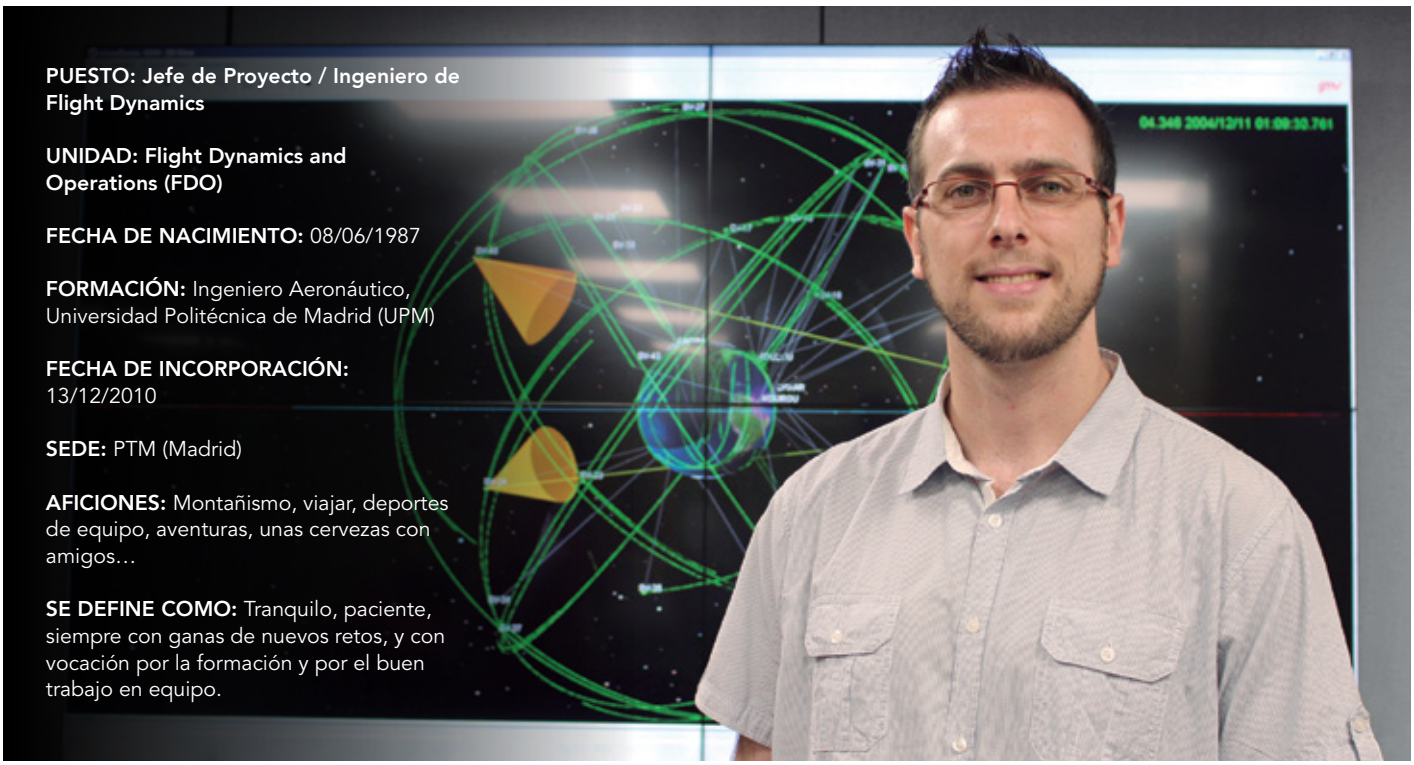
ANTONIO LOZANO LIMA

"Las becas de GMV están llenas de oportunidades, tanto para la empresa como para los estudiantes"

En verano de 2009, cuando todavía tenía un curso por delante para terminar la universidad, estaba estudiando la especialidad de aeropuertos, que era la que siempre me había gustado, y nunca me había planteado trabajar en espacio. Pero por otro lado, me parecía fundamental conocer el entorno de la empresa antes de terminar la carrera, y no quería encerrarme en mi especialidad demasiado pronto. Y así, buscando trabajos de verano por distintas ramas de la aeronáutica, aterricé aquí por un anuncio que vi en un tablón de la universidad.

Aún me sorprende que dos meses a media jornada fuesen suficiente para cambiar mis preferencias maduradas durante varios años, pero aquí encontré algo distinto, algo más allá de un trabajo interesante. Había sin duda un gran ambiente, estábamos en medio de un equipo de gente joven trabajando con ilusión, y se veía que las cosas funcionaban con suavidad a todos los niveles de la empresa. En su momento no conocía todo el trabajo que hay detrás de eso, pero sí que intuí que había muchas cosas que merecían la pena.

Antonio Lozano con el grupo de becarios 2017



PUESTO: Jefe de Proyecto / Ingeniero de Flight Dynamics

UNIDAD: Flight Dynamics and Operations (FDO)

FECHA DE NACIMIENTO: 08/06/1987

FORMACIÓN: Ingeniero Aeronáutico, Universidad Politécnica de Madrid (UPM)

FECHA DE INCORPORACIÓN: 13/12/2010

SEDE: PTM (Madrid)

AFICIONES: Montañismo, viajar, deportes de equipo, aventuras, unas cervezas con amigos…

SE DEFINE COMO: Tranquilo, paciente, siempre con ganas de nuevos retos, y con vocación por la formación y por el buen trabajo en equipo.

Las becas nos permiten cambiar un poco la rutina y hacer pequeñas investigaciones en nuevas áreas

Además de todo el contexto que daba GMV, la beca en sí misma fue una gran experiencia. Llegas con el tópico en la cabeza de hacer fotocopias y poner cafés al jefe, o como poco estar en un rincón aburrido. Pero en lugar de eso ves que desde el primer día ya te han preparado todo, te hacen presentaciones sobre la empresa, te ofrecen varios temas de trabajo para que puedas elegir, y luego tienes a unos tutores volcados contigo. Realmente fue una vivencia profesional y personal fantástica. Animado por mis tutores y por la buena experiencia, durante el último curso de la universidad continué como becario haciendo el proyecto fin de carrera. Finalmente, cuando se acercó el momento de graduarme y buscar mi primer trabajo, la decisión estaba clara: quería entrar en GMV.

Entré en el departamento de FDO (*Flight Dynamics and Operations*), donde sigo trabajando a día de hoy, haciendo software de dinámica orbital. Entre otras muchas cosas interesantes, este trabajo me ha dado la oportunidad de trabajar con gente de varios países, de colaborar en el análisis de misión de los satélites de nuestros clientes, así como de participar en varios lanzamientos de satélites desde el centro de control de misión. Aparte del trabajo, siempre que puedo me gusta apuntarme a los deportes que se organizan en GMV (fútbol, baloncesto, vóley…) donde siempre te lo pasas bien, haces algo de ejercicio, y conoces a compañeros de otros departamentos.

Pasados unos años, se me ofreció la posibilidad de ser tutor de una beca y no lo dudé ni un momento. Las becas nos permiten cambiar un poco la rutina y hacer pequeñas investigaciones en nuevas áreas, lo cual es sin duda muy atractivo. Por otro lado, también es una gran oportunidad para la empresa para conocer buenos candidatos para futuras vacantes. Pero para mí, es además la oportunidad de continuar la labor de dar conocer GMV y transmitir todas aquellas cosas positivas que me convencieron para querer quedarme. Desde entonces he tenido la suerte de ser tutor de varias becas en la empresa, trabajando con ya más de 10 estudiantes, de varias carreras y universidades, y cada instante dedicado a ellos ha merecido la pena. Muchos de ellos son ahora mis compañeros y amigos en GMV, y espero que sean muchos más en los próximos años.

GMV EN EL MUNDO

ALEMANIA
GMV Insyen AG.
- Münchener Straße 20 - 82234 Weßling
  Tel.: +49 (0) 8153 28 1822 Fax: +49 (0) 8153 28 1885

- Friedrichshafener Straße 7 - 82205 Gilching
  Tel.: +49 (0) 8105 77670 160 Fax: +49 (0) 8153 28 1885

- Europaplatz 2, 5. OG, D-64293 Darmstadt
  Tel.: +49 (0) 6151 3972970 Fax: +49 (0) 6151 8609415

COLOMBIA
Edificio World Trade Center Bogotá - Calle 100 No. 8A-49. Torre B. PH.- Bogotá
Tel.: +57 (1) 6467399 Fax: +57 (1) 6461101

EE.UU
2400 Research Blvd, Ste 390 Rockville, MD 20850
Tel.: +1 (240) 252-2320 Fax: +1 (240) 252-2321

523 W 6th St Suite 444 Los Angeles, California 90014
Tel.: +1 (310) 728-6997 Fax: +1 (310) 734-6831

ESPAÑA
Isaac Newton 11 P.T.M. Tres Cantos - 28760 Madrid
Tel.: +34 91 807 21 00 Fax: +34 91 807 21 99

Juan de Herrera nº17 Boecillo - 47151 Valladolid
Tel.: +34 983 54 65 54 Fax: +34 983 54 65 53

C/ Albert Einstein, s/n 5ª Planta, Módulo 2, Edificio Insur Cartuja - 41092 Sevilla
Tel.: +34 95 408 80 60 Fax.: +34 95 408 12 33

Balmes 268-270 5ª Planta - 08006 Barcelona
Tel.: +34 93 272 18 48 Fax: +34 93 215 61 87

C/ Mas Dorca 13, Nave 5 Pol. Ind. L'Ametlla Park L'Ametlla del Vallés - 08480 Barcelona
Tel.: +34 93 845 79 00/10 Fax: + 34 93 781 16 61

Edificio Sorolla Center, Av. Cortes Valencianas nº58, local 7 - 46015 Valencia
Tel.: +34 96 332 39 00 Fax: +34 96 332 39 01

Avenida José Aguado, 41 - Edificio INTECO, 1ª Planta - 24005 León
Tel.: +34 91 807 21 00 Fax: +34 91 807 21 99

Parque Empresarial Dinamiza, Av. Ranillas 1D - Edificio Dinamiza 1D, planta 3ª, oficinas B y C
50018 Zaragoza
Tel.: 976 50 68 08 Fax: 976 74 08 09

FRANCIA
17, rue Hermès - 31520 Ramonville St. Agne. Toulouse
Tel.: +33 (0) 534314261 Fax: +33 (0) 562067963

MALASIA
Level 8, Pavilion KL 168, Jalan Bukit Bintang, 55100 Kuala Lumpur
Tel.: (+60 3) 9205 7788 Fax: (+60 3) 9205 7788

POLONIA
Ul. Hrubieszowska 2, 01-209 Varsovia
Tel.: +48 22 395 51 65 Fax: +48 22 395 51 67

PORTUGAL
Avda. D. João II, Nº 43 Torre Fernão de Magalhães, 7º 1998-025 Lisboa
Tel.: +351 21 382 93 66 Fax: +351 21 386 64 93

REINO UNIDO
Harwell Innovation Centre, Building 173, 1st floor, suite C131 & C134 Curie Avenue, Harwell
Science and Innovation Campus, Didcot, Oxfordshire OX11 0QG
Tel.: +44 1235 838536 Fax: +44 (0)1235 838501

RUMANIA
SkyTower, 246C Calea Floreasca, 32nd Floor, District 1, postal code 014476, Bucharest
Tel.: +40 318 242 800 Fax: +40 318 242 801