News

N° 77

gmv INNOVATING SOLUTIONS

Ciberseguridad a la altura de las circunstancias

ENTREVISTA
Guillermo Llorente Ballesteros
Director corporativo de Seguridad de MAPFRE

ISO 27701
Gestión sostenible de la privacidad

La economía experimenta un proceso de transformación digital sin precedentes. Un aspecto clave de este proceso es la explotación masiva de datos para la definición de estrategias y modelos de negocio centrados en el cliente (*data-driven customer-centric*).

En este contexto, la protección de los datos personales cobra una especial relevancia no sólo por ser una obligación legal (RGPD, LGLP, CCPA, etc.), sino porque la vulneración de la privacidad puede traducirse en una merma de confianza que se materialice en un impacto de negocio.

Sin embargo, garantizar la privacidad o dar cumplimiento a los requisitos regulatorios no es una tarea trivial. Factores como la velocidad de cambio, la complejidad de los entornos, la escala de los procesos de negocio, etc. hacen que los costes asociados crezcan de forma exponencial con aproximaciones parciales e ineficientes.

Se impone la necesidad de definir un modelo de gestión de la privacidad sostenible.

marketing.TIC@gmv.com

gmv
INNOVATING SOLUTIONS

Carta de la presidenta

Recientemente abrí un fichero que recibí por correo electrónico. Leí el correo de pasada y le dí al archivo adjunto. Podía haber sido un virus, un *ransomware* o cualquier otro tipo de programa malicioso, pero afortunadamente era un mensaje de concienciación.

Desde hace ya más de un cuarto de siglo, GMV desarrolla servicios y soluciones que permiten diagnosticar el nivel de ciberseguridad, gestionar las infraestructuras tecnológicas y gobernar el proceso de ciberseguridad de sus clientes. La necesidad de defenderse frente a ataques cibernéticos es común a todo tipo de sistemas interconectados pero dispares, que requieren de soluciones adaptadas a cada caso. GMV cuenta con una amplia experiencia y soluciones específicas, tanto para proteger las redes corporativas de grandes empresas, como para cajeros automáticos, servicios médicos, sistemas industriales, o centros de control de satélite.

Este año que llevamos de pandemia ha demostrado contundentemente que la digitalización no sólo permite mejorar la productividad y usar los recursos de forma más eficiente, además ha permitido a muchas empresas continuar su actividad a pesar del confinamiento a través del teletrabajo. Por otro lado, el teletrabajo conlleva un incremento importante de vulnerabilidad a ciberataques a empresas y organismos públicos, que de hecho han aumentado notablemente durante la pandemia; al igual que los ataques a particulares, consecuencia de que también gran parte de nuestra vida social ha pasado a modo virtual. Tanto en un caso como en otro es necesario que los usuarios nos concienciemos y sepamos identificar situaciones de riesgo en este entorno. Porque la ciberseguridad es una carrera tecnológica contra el cibercrimen en la que el ser humano con frecuencia es el punto más débil.

Mónica Martínez

N° 77

Edita
GMV

Dirección-Coordinación
Marta Jimeno, Marta del Pozo

Responsables de área
Antonio Hernández, Miguel Ángel Molina, José Prieto, Javier Zubieta

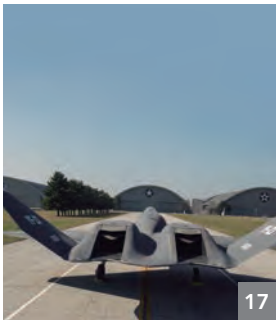
Redacción
Alberto Águeda, Luis Javier Álvarez, António Araújo, Carlos Barredo, Mariano J. Benito, Filipe Brandão, Antonio Cabañas, Francisco Cabral, María Jesús Calvo, Jesús Cegarra, Maole Cerezo, Ana Cezón, Cristian Corneliu, Luis Manuel Cuesta, Marco Donadio, Iulia Dragomir, Raquel Fernández, Teresa Ferreira, Javier Fidalgo, Alberto de la Fuente, Hugo Garzón, Javier Gómez, Mariella Graziano, Sara Gutiérrez, Juan Ramón Gutiérrez, Sergi Güell, Ana Herrera, Filipe Henriques, Héctor Herrero, Javier Hidalgo, Aurora Izquierdo, Rafał Krzysiak, Cristina Liébana, Fátima López, Jesús Alejandro López, Arturo Martín, David Merino, Carlos Molina, Daniel Montero, Cristina Muñoz, Héctor Naranjo, Jorge Ocón, Eric Polvorosa, Isidro Prieto, José Prieto, Beatriz Revilla, Pablo Rivas, Eugenio Sillero, Antonio Tabasco, Tatiana Teresa, Maria Victoria Toledano, Manuel Toledo, João Vitorino

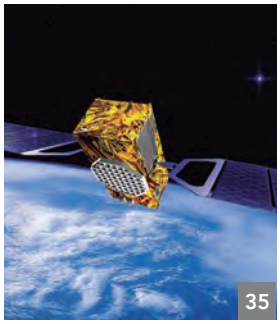
Arte, diseño y maquetación
Paloma Casero, Verónica Arribas

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

Revista N°. 77 - 1er Trimestre de 2021

CONTENIDOS





Ciberseguridad a la altura de las circunstancias

Tras la irrupción del coronavirus podemos afirmar que nos encontramos ante un nuevo escenario a nivel mundial que ha cambiado de manera profunda nuestra forma de socializar, de ver las cosas, de priorizar y, por supuesto, de trabajar. Es muy probable que cuando todo esto pase, volvamos a una situación parecida a nuestra vida anterior. También es muy probable que actividades que ahora hacemos por obligación o necesidad, como el teletrabajo, se consoliden en nuestro día a día ya que durante estos meses se está mostrando como una alternativa beneficiosa.

La ciberseguridad, en cada una de sus facetas, ha demostrado su aportación positiva a todos los niveles y todo hace pensar que «ha puesto una pica en Flandes» en este proceso acelerado de digitalización que estamos viviendo como sociedad. Son varios los factores que han contribuido a ello y se abordan a continuación.

Uno de los más impactantes en la esfera personal ha sido la irrupción abrupta de una nueva forma de trabajar absolutamente deslocalizada, que acabamos denominando «teletrabajo», aunque en el contexto de la pandemia está siendo mucho más exigente que el teletrabajo tal y como lo entendíamos antes de ella.

Cuando la necesidad de quedarse en casa trabajando surgió, no nos sorprendió por igual a todos. GMV ha constatado que aquellas compañías con un sistema de continuidad de negocio ya rodado han estado mejor preparadas. Por ejemplo, en los meses de enero y febrero de 2020 cuando ya se vislumbraba lo que iba a suceder, algunas empresas pudieron poner en marcha el plan de continuidad para, por ejemplo, realizar pruebas de estrés ante un elevado número de teletrabajadores, hacer un determinado acopio de material o redoblar las actividades de pruebas de contingencias tecnológicas. Esta mejor preparación ha posibilitado que el impacto fuese menor y, como consecuencia, la resiliencia superior.

Además, varios de los clientes a los que GMV presta servicio estaban en la misma situación de preestado de alarma, por lo que fue posible retroalimentarse mutuamente de las prácticas que todos estábamos desplegando. Por ejemplo, tanto GMV como varios de sus clientes prefirieron pasar a teletrabajo ciertas, actividades antes de que se decretara el estado de alarma, incluso antes de que se cerraran los colegios. Algo que a nivel familiar fue tremendamente impactante.

Por lo tanto, compensa apostar por la implantación de sistemas de gestión definidos por estándares de manera general y, en este caso específico por el de la continuidad de negocio. Ciberseguridad a la altura de la circunstancias.

TELETRABAJO SEGURO

En la nueva situación, GMV ha sido consciente de que el denominado «perímetro corporativo» saltaba por los aires, pasando a formar parte de ese perímetro el *router* particular del trabajador. Esto provocó una inquietud inicial aunque, según pasaban las semanas, se demostró que la ciberamenaza estaba más presente en otros escenarios.

Desde una perspectiva tecnológica, las organizaciones han podido aplicar muchas medidas de ciberprotección a la infraestructura tecnológica sobre la que se sustenta el teletrabajo. Este hecho no ha impactado de la misma manera a todas las organizaciones, ya que muchas de ellas han constatado carencias importantes debido a la existencia y persistencia de vulnerabilidades. Para aquellas organizaciones que restaron importancia a la ciberseguridad durante el despliegue del teletrabajo, ahora mismo es un buen momento para llevar a cabo esas revisiones y acometer mejoras. La inversión en gestión de vulnerabilidades siempre tiene su retorno.

Por lo tanto, teletrabajar con ciberseguridad incorporada es compatible, complementario y necesario. Ciberseguridad a la altura de las circunstancias.

CIBERAMENAZAS SIEMPRE LATENTES

Podemos destacar dos escenarios donde las ciberamenazas están siendo especialmente virulentas en esta pandemia. El primero, el ámbito corporativo, que ha sufrido importantes oleadas de ataques *ransomware*, y, aunque podríamos denominarlo cibercriminalidad «business as usual», el impacto de éstos ha sido superior que en otras ocasiones. En este 2021, económicamente incierto, se debería tener presente que hay desinversiones que pueden salir muy caras incluso a corto plazo, ya que los ciberdelincuentes demuestran su capacidad de llegada. Lo último que se necesita es tener que lidiar con paradas de servicio o robo de información.

El segundo escenario se circunscribe al ámbito particular. La ciberseguridad suena como algo difícil y tecnológico para cualquiera que no se dedique a ello y, aderezado con mensajes de amenazas y miedo, es el cóctel perfecto para que los particulares no le hagan mucho caso hasta que no padezcan un ciberincidente. No es casual, por tanto, la proliferación en estos tiempos de campañas masivas de *phishing* a través de email, SMS o *WhatsApp* con ganchos de todo tipo para que el usuario haga clic donde no debe. Como contrapartida, gracias a que nuestra exposición digital ha crecido tanto, estamos mejor informados y podemos acceder a conocimiento sobre ciberseguridad con más facilidad. Un ejemplo de ello ha sido la gran cantidad de sesiones formativas que se han impartido de forma virtual y gratuita en estos meses, además de material educativo accesible y de calidad a disposición de los particulares. Este esfuerzo en capacitar y sensibilizar no se había visto antes. Ciberseguridad a la altura de las circunstancias.

CIBERSEGURIDAD EN SALUD

La irrupción de la pandemia y sus sucesivas olas protagonizaron muchas consultas en internet. La sociedad estaba ávida de conocimiento acerca de un virus que provocaba episodios de salud graves e incluso la muerte. A la vez, el sistema sanitario entró en situaciones de estrés que afectaron tanto a su capacidad hospitalaria como al equilibrio emocional de los sanitarios que se referían a la situación que estaban viviendo como «de guerra».

Si ya de por sí los datos sanitarios figuraban antes de la pandemia entre los de tráfico más rentable en el mercado negro —disputándose

el primer lugar del volumen de negocio con los datos bancarios y los personales o de identidad en redes sociales— las organizaciones que los generan y custodian, quedaron aún más expuestas al interés de los ciberdelincuentes. De hecho, importantes corporaciones que operan en el sector de la salud y hospitales han sufrido incidentes en este ámbito.

Ha transcurrido más de un año desde que presenciáramos las imágenes a cámara rápida de la construcción de un megahospital prefabricado en China. A las puertas de la inmunidad, gracias al esfuerzo realizado por investigadores e industria farmacéutica, comenzamos a familiarizarnos con otro concepto antes desconocido para la mayoría: la fatiga pandémica.

A la preocupación inicial que generó la llegada a nuestras vidas del virus se suma el anhelo de ser vacunados y la fatiga que ocasionan meses de mascarilla, inquietud por la proliferación masiva de enfermos y fallecidos, confinamiento domiciliario, cierres perimetrales, telediarios y programas con el SARS-CoV-2 como monotema. Todo ello ha configurado un estado de vulnerabilidad que continúan explotando ciberdelincuentes sin escrúpulos.

SIN PERDER TIEMPO

El 23 de marzo de 2020, en pleno cierre total de España, la Policía Nacional informaba que había detectado un intento de bloquear los ordenadores de los hospitales españoles mediante el envío a los sanitarios de correos electrónicos con un «virus muy peligroso», cuyo objetivo era vulnerar el sistema informático de los centros médicos.

Un reflejo de la preocupación que genera una potencial indisponibilidad de los sistemas de nuestros hospitales, es la pregunta parlamentaria que tuvo que responder el Ministerio del Interior el pasado mes de octubre: «En lo que va de 2020, el Centro Nacional de Protección de Infraestructuras y Ciberseguridad (CNPIC) ha tenido conocimiento de tres graves ciberincidentes en materia sanitaria, uno de ellos dirigido a un operador crítico». Cabe destacar que, según datos de un reciente informe de Check Point Research, España es el tercer país con mayor grado de ciberinfección, sólo por detrás de Canadá y Alemania.

A nivel mundial, otro hecho significativo fue la carta de la Cruz Roja rubricada por personalidades de la empresa y la política como los presidentes de Telefónica o Microsoft o ex presidentes de Brasil y Colombia e ideada por el Instituto CyberPeace (organización sin ánimo de lucro impulsada por Microsoft, la Fundación Hewlett, MasterCard y otras grandes corporaciones e instituciones con el objetivo de proteger a las víctimas contra los ataques cibernéticos y ayudarlos a recuperarse tras él). En ella se instaba a los gobiernos a reconocer que «las operaciones cibernéticas contra los centros de salud son ilegales e inaceptables» y a que trabajasen junto a la sociedad civil y el sector privado para que las instalaciones médicas sean respetadas y protegidas. «No toleramos ataques a la infraestructura de salud en el mundo físico y no debemos tolerar tales ataques en el ciberespacio», rezaba el escrito. Cabe destacar que, a nivel mundial, los ataques dirigidos contra empresas del sector salud se han incrementado en un 45 % desde la irrupción de la pandemia.

NUESTRO COMPROMISO

GMV, consciente de los potenciales peligros y como proveedor de referencia de servicios gestionados de seguridad desde su Centro de Respuesta ante Incidentes de Seguridad Informáticas GMV-CERT, ha sumado los esfuerzos de su Equipo de Inteligencia de Ciberamenazas a la lucha contra la ciberdelincuencia en el sector de

la salud en nuestro país, ya que monitoriza permanentemente la actividad maliciosa. Como resultado de esta vigilancia y del comportamiento observado durante las dos primeras olas de contagios en nuestro país, la compañía publicó el informe «Ciberamenazas susceptibles de afectar al sistema sanitario español», en el que advertía del riesgo de ciberataques a proveedores de servicios sanitarios, compañías farmacéuticas, aseguradoras y centros sanitarios. Los últimos ataques de *ransomware* detectados pusieron al descubierto que el objetivo principal de estos ciberdelincuentes era el robo de datos relacionados con la información de las historias clínicas de pacientes, del personal sanitario, información sobre el desarrollo de nuevos medicamentos, ensayos clínicos, la propiedad industrial, etc.

En este informe se alertaba ya en abril que «entre el 60 y el 70 % de las amenazas tenían como vector de entrada la ingeniería social. Los *hackers* aprovechan la debilidad humana, apelando a la necesidad de información, la curiosidad, el temor o el altruismo respecto a la COVID-19». Asimismo, en el mencionado informe, GMV incluía una batería de recomendaciones para que proveedores de servicios sanitarios, compañías farmacéuticas, aseguradoras y centros sanitarios se mantengan en alerta frente a posibles amenazas.

DESDE NUESTRA ATALAYA

Cuando la vacuna ya se ha inoculado en residencias entre sanitarios y cuerpos de seguridad del Estado y otros colectivos prioritarios, sorteamos a fecha de hoy una nueva ola y los efectos de nuevas cepas de un virus que ya ha causado más de 2,6 millones de muertes en todo el mundo. Por otra parte, la falta de información sobre un calendario de vacunación para toda la población y la convulsión política que se vive en el momento en que escribimos el reportaje, según los expertos de GMV, conforman un terreno fértil para los grupos de ciberdelincuencia organizada.

Los resultados de la monitorización que realiza el Equipo de Inteligencia de GMV, en lo que llevamos del presente año 2021, vienen corroborando la anterior afirmación. Identificamos desde campañas para acceder a los domicilios de personas mayores hasta la infiltración de *malware* en instituciones sanitarias y en otras vitales para el contexto económico que estamos viviendo así como intentos de sabotaje contra la cadena de suministro.

Durante este último año 2020 se ha podido observar un aumento en los ataques al sector de la sanidad y en las administraciones públicas. Además, el impacto de la COVID-19 en el plano digital se ha propagado por el mundo y particularmente en España se ha producido un incremento sustancial con respecto al año anterior de fraudes y estafas *online*.

Organismos de la administración pública como la Seguridad Social, la Agencia Tributaria o la DGT, entre otros, han sido muy utilizados para la suplantación de su identidad con el propósito de cometer fraude o distribuir *malware*. Otros han sufrido graves incidentes llegando incluso a paralizar su actividad debido al cifrado de los datos por ataques *ransomware*. El panorama de la seguridad a nivel mundial debería preocupar no solo a los profesionales y empresas que nos dedicamos a ello porque a una industria de la ciberdelincuencia, cada vez mejor armada, se suman las vulnerabilidades halladas en sistemas utilizados por grandes empresas y entidades oficiales como los casos de SolarWinds, VMWARE o las de los servidores Exchange de Microsoft. Todo ello nos hace presagiar que se agravará la situación durante el año 2021.

Juan Ramón Gutiérrez, jefe de la sección de Inteligencia de Amenazas y Forense. Secure e-Solutions de GMV

MONITORIZACIÓN CONTINUA

En este escenario convulso, el *ransomware* se convierte en la mayor preocupación de las organizaciones debido a su facilidad para obtener versiones «as a service» en el mercado negro. También porque cada vez actúan con mayor agresividad, siendo las campañas de *phishing, smishing* y cualquier método de mensajería electrónica la manera más rápida, eficiente e incluso barata de distribución, ya que aplican estrategias de ingeniería social que persiguen engañar a los usuarios con mensajes que despierten su curiosidad, temor u otro sentimiento relacionado con el SARS-CoV-2 y las vacunaciones.

Con la perspectiva que nos ofrece el Equipo de Inteligencia de Amenazas en la monitorización del ciberespacio y el seguimiento de internet, nos atrevemos a confirmar que la vacunación es a día de hoy el tema de preocupación mundial y, como ya se está haciendo patente, el flanco que más utilizará la cibercriminalidad para actuar, no desestimando otros relacionados directamente con la pandemia, como las subvenciones destinadas a paliar sus estragos económicos. Al mismo tiempo persistirán los intentos de ciberfraude vía mensajes (SMS, email, *WhatsApp*) relacionados con la entrega de paquetería. Si bien durante el pasado año se produjo un aumento exponencial de las compras por internet, este parece que continúa en ascenso, incrementándose las oportunidades para los ciberdelincuentes.

Uno de los aspectos más sensibles en el flanco de las vacunas es la cadena de suministros (Laboratorios / Logística / Centros de Vacunación / Hospitales) en el que aumentan las amenazas. Se utilizan argumentos de ingeniería social para perpetuar ataques contra cualquiera de los actores de dicha cadena, observándose acciones de suplantación de identidad de algún actor de la misma para favorecer la infección de los sistemas de información del resto. Recordemos que hablamos de datos críticos para la vida humana de muy alto valor y que pueden ser, por tanto, objeto de chantaje mediante peticiones de rescate como de venta en los mercados negros.

En 2021 entran en escena nuevos actores (no quiere decir que no existiesen antes) en el teatro de operaciones de las ciberamenazas. La aparición de las diferentes vacunas a nivel internacional, amparadas por los distintos bloques (EE. UU, Europa, Rusia y China), amplía el espectro a intereses incluso supranacionales, económicos y políticos. En definitiva, las vacunas ofrecen una serie de oportunidades de posicionamiento geoestratégico que seguramente ningún bloque querrá perderse.

REFORZAR NUESTROS SISTEMAS DE DEFENSA

Entre las medidas más eficaces para protegernos figura la detección temprana, ya que correlaciona los datos obtenidos por la inteligencia de amenazas con las vulnerabilidades que ofrece tanto el perímetro como los activos internos de la organización. A este factor hay que sumarle la imprescindible concienciación permanente de los usuarios, ya que una vez que el artefacto (*malware/ ransomware*) ha infectado una máquina del interior de la organización, los sistemas convencionales de monitorización únicamente pueden identificar para su contención aquellas que están siendo infectadas debido a la rapidez con la que se produce el contagio entre equipos de la red (movimientos laterales).

Hay que tener en cuenta que el actual *ransomware* tiene una «fase explosiva» o momento en el que de manera repentina aparecen multitud de ordenadores infectados, habiéndose producido la propagación de forma silenciosa y evadiendo las medidas de detección. De ahí su peligrosidad y la importancia de la inteligencia de amenazas como medida preventiva que nos permita obtener una ventaja táctica frente a la cibercriminalidad.

Al igual que en la pandemia de la COVID-19 (o cualquier otra de tipo biológico) las infecciones de sistemas informáticos (digitales) tienen su «paciente 0» y, a partir de él, su capacidad de propagación (movimientos laterales) es ilimitada si no se toman medidas de contención. Este hecho explica la relevancia que tienen las campañas de *phishing* como vector principal en la infección de sistemas digitales y la insistencia de no abrir ninguna notificación o aviso extraño con carácter alarmista que pudiese llegar por correo electrónico, mensaje de wassap o cualquier otro tipo de mensajería electrónica incluyendo los mensajes cortos (SMS).

En caso de dudas, antes de abrir cualquier enlace dentro del mensaje o archivo adjunto, primero hay que tomarse el tiempo necesario para comprobar con otras fuentes la veracidad de estos mensajes porque nunca la administración pública ni nuestro banco nos pedirán interactuar con ellos utilizando la mensajería.

No cabe duda de que la conjunción de los vectores «COVID-19» y «vacuna» suponen ya la principal oportunidad para la delincuencia organizada como se hace patente en infinidad de artículos de sucesos relacionados con incidentes de ciberseguridad y con la sofisticación en los métodos del engaño. La suplantación de la identidad de servicios de confianza para engañar a usuarios, ya sean particulares o de organizaciones y empresas, será la tónica que veremos repetida en 2021.

Conocemos demasiados ejemplos de ataques que paralizan toda la actividad de la organización que lo sufre y, en muchos casos, genera una importante alarma social de la que se hacen eco los medios de comunicación de todo el país. Como en el cuento de Caperucita Roja, los expertos venimos avisando de la llegada del lobo, pero han de suceder hechos de esta naturaleza para que se comprenda que, en materia de ciberseguridad, no hablamos de cuentos.

Guillermo Llorente Ballesteros

Director corporativo de Seguridad de MAPFRE

Es Teniente Coronel de Infantería, Diplomado de Estado Mayor y Estado Mayor Conjunto en situación de excedencia.

Tras ocupar diversos destinos al mando de unidades y participar en numerosas misiones internacionales, llega al campo de la seguridad en su empleo de Comandante, ocupando durante seis años el puesto de jefe de la Unidad de Contrainteligencia, Seguridad Interior y del Personal del Ejército de Tierra, estando en posesión de diversas condecoraciones.

En el año 2006 se incorporó a MAPFRE, siendo actualmente director corporativo de Seguridad de MAPFRE, con responsabilidad global sobre todas las áreas de seguridad tanto en el ámbito lógico como en el ámbito físico o de las instalaciones, la continuidad de negocio y gestión de crisis, o la privacidad de los datos personales.

El modelo integral de seguridad del Grupo MAPFRE ha sido considerado caso de éxito por la consultora tecnológica Gartner y ha recibido numerosos premios y distinciones por su carácter innovador, entre otros, así como el primer premio de la Guardia Civil «Duque de Ahumada a la Excelencia en Seguridad Corporativa».

Es ponente habitual en coloquios y conferencias, así como profesor de diversos másteres y cursos de posgrado de diferentes universidades en materias relacionadas con la seguridad.

Has sido uno de los grandes evangelizadores en cuanto a la conveniencia de establecer sinergias entre los ámbitos de la seguridad física y lógica. ¿Cuál es tu perspectiva de la convergencia entre ambas?

La esencia de nuestro modelo de seguridad es que sitúa al «cliente» en el centro de nuestra atención, con objeto de brindarle una protección homogénea y consistente frente a cualquier tipo de amenazas, con independencia de cuál sea la dimensión en que estas se desarrollan.

Este modelo aporta un número significativo de beneficios. El primero es que favorece la obtención de sinergias entre las medidas destinadas a cubrir los diferentes vectores de ataque o dimensiones de seguridad. El segundo es que favorece la homogeneidad del modelo de protección, evitando que haya desigualdad o incoherencia entre las medidas adoptadas en los diferentes ámbitos.

Asimismo, este abordaje global favorece dos procesos clave en materia de seguridad: el de planificación, y el de monitorización y respuesta a la crisis. Con esta perspectiva creo que es posible definir más eficientemente el modo, momento y con qué fortaleza, debemos aplicar los esfuerzos para prevenir el ataque. Tener una visión global nos ha permitido ser capaces de coordinar la respuesta a la crisis moviendo las palancas de cada uno de los vectores de una forma homogénea y coordinada y también concurrente a este fin. No tiene sentido dar una respuesta independiente en cada uno de los vectores cuando la amenaza utiliza en su ataque varias dimensiones simultáneamente.

Como conclusión, en mi opinión, solamente mediante la integración de los mundos físico y lógico y de la información obtenida de ellos, seremos capaces de dar una protección eficaz y eficiente a las nuevas amenazas.

Este enfoque supone un reto tecnológico, trabajar con diferentes fuentes de información del mundo físico y lógico. ¿Cómo estamos de preparados desde el punto de vista de las corporaciones?

Desde nuestra posición vemos que a las corporaciones en general nos queda un largo camino por delante y con un alto grado de incertidumbre en lo que se refiere a la mejor solución para la integración de la información de los diferentes sistemas. No solo en lo relativo a la integración de elementos del mundo físico y lógico, que si bien hay una parte que está solventada (como la de los *logs* de las cámaras de vídeo, de los pasos de tarjeta, etc., hay otros ámbitos aún pendientes) sino también al propio mundo digital, donde asimismo afrontamos retos formidables como la gestión y centralización de la información obtenida de las diferentes nubes de los diferentes fabricantes de forma eficiente. La migración a entornos *cloud* ha añadido complejidad a la ya existente que, por cierto, era ya de por sí elevada.

Siendo MAPFRE una compañía global, con una importante huella internacional, ¿qué retos de seguridad os plantea esta dispersión geográfica y cómo los estáis abordando?
MAPFRE tiene presencia en casi medio centenar de países. Este hecho, si bien resulta un activo fundamental por la riqueza que aporta a todo el grupo, desde el punto de vista de la seguridad supone un desafío muy importante. Asimismo, esta dispersión geográfica conlleva retos de magnitud para los equipos de gestión.

La dificultad principal que entraña nuestra presencia global, estriba en ser capaces de proporcionar una seguridad homogénea a nuestros compañeros y a nuestra red, con independencia de la localización de los activos y de los sistemas de la información. Es un reto al que no podemos esquivar la mirada, tenemos obligatoriamente que hacerle frente con enorme decisión.

Y en su consecución hemos de ser capaces de mantener un equilibrio con el mantenimiento de la flexibilidad suficiente para poder responder a las particularidades locales, que no podemos obviar, como la velocidad de adaptación de los equipos humanos, su tamaño, las diferentes idiosincrasias y culturas o las propias actividades de negocio a que se orienta cada compañía. Todo ello añade un nivel mayor de complejidad a un reto, que ya es de enorme dimensión.

Por último, junto a la necesidad de establecer un estándar homogéneo y la capacidad de ser flexibles para adaptarnos a distintos escenarios, nos encontramos con un apartado que complica aún más nuestra actividad: una legislación, cada vez más prolija y propia de cada país donde MAPFRE tiene presencia.

En el modelo de MAPFRE la seguridad forma parte de la vida de la organización en todas sus dimensiones

¿Qué papel tiene el área de seguridad dentro de la organización de MAPFRE? ¿Qué servicios se demandan desde el resto de la organización al departamento de seguridad?
Nuestro concepto es que la seguridad es parte intrínseca de la organización y debe estar implicada e integrada en la vida y el funcionamiento ordinario de ésta. No cabe desempeñar un papel relevante solo en situaciones de crisis, los departamentos de seguridad tenemos que formar parte de la corriente subyacente que mueve la organización y no quedarnos en la superficie.

En el modelo de MAPFRE, del que estamos satisfechos y orgullosos, la seguridad forma parte de la vida de la organización en todas sus dimensiones. Esto propicia que nos sintamos un eslabón relevante de la organización y favorece nuestro alineamiento con la estrategia global. Además, nos faculta para dotar a cada una de las iniciativas impulsadas de una seguridad eficiente, ya que al integrarla desde el diseño de cualquier nueva iniciativa o proyecto resulta más sencillo y barato proporcionársela que una vez que ya están en marcha.

¿Veis una demanda activa de servicios del resto de la compañía? ¿Qué nivel de demanda percibís?
La demanda interna no ha parado de crecer, acentuándose en los últimos cinco años debido a dos factores fundamentales. El primero, que el conjunto de la compañía ha tomado conciencia en mayor medida de la importancia de la seguridad, fruto de los programas y planes de formación internos que hemos puesto en marcha. El segundo, que la sociedad en su conjunto es cada vez más consciente de su relevancia. Hechos como la entrada en vigor del GDPR (*General Data Protection Regulation*) ha supuesto un cambio de dimensión en la sensibilización de los ciudadanos sobre aspectos relacionados con la privacidad y protección de datos.

Estos dos factores, la mayor conciencia interna y el estado de opinión generado tanto por los medios de comunicación como por otros *stakeholders* (auditores, grupos de interés, etc.), han contribuido al incremento de la demanda de seguridad en cualquier proyecto de forma natural.

Por nuestra parte, hemos sido capaces de responder a las demandas de nuestros compañeros. Hemos sido receptivos a las necesidades, actuando como facilitadores de su trabajo siempre con el objetivo de proporcionar seguridad, siendo responsables con el medioambiente y cumpliendo las leyes. Demanda que ha crecido permanentemente como respuesta a todo lo anteriormente expuesto, lo que nos hace sentir satisfechos de cómo estamos integrados en la vida de la compañía.

¿Qué iniciativas en el ámbito de la ciberseguridad destacarías por su relevancia?
Actualmente, el mayor reto al que nos enfrentamos es poder aumentar nuestra capacidad de monitorización y respuesta de los entornos *cloud*. La compañía tiene un principio en materia tecnológica que es «cloud first». Bajo esa premisa, el proceso de transformación digital y de migración hacia entornos *cloud* ha de convivir, necesariamente y de forma ineludible, con una realidad «on premise» que no va a desaparecer, que tiene un crecimiento vegetativo propio y soporta aún procesos críticos para la compañía.

En este modelo de convivencia, hemos de potenciar de forma decidida y a corto plazo nuestras capacidades de monitorización y respuesta sobre los activos ubicados en *cloud*, que no van a parar de crecer y que requieren un nivel de seguridad acorde a los riesgos actuales. El desafío está en encontrar la manera de implantarlo de una forma eficiente.

En este momento la ciberseguridad es un área en la vanguardia del conocimiento. El libro de cómo hay que hacer las cosas en cada uno de los entornos no está escrito. La situación actual nos demanda dar seguridad en un contexto de alta volatilidad y una complejidad tecnológica enorme.

La pandemia ha supuesto una vuelta de tuerca a esta complejidad que mencionas. ¿Cómo ha afectado esta etapa en MAPFRE bajo el punto de vista de la ciberseguridad? Personalmente, ¿cómo lo has vivido estos últimos meses?

Coincidiremos en que esta pandemia es un drama global, tanto humano como económico, y no podemos olvidar los millones de personas que han fallecido a causa de la COVID-19. Sin olvidar nunca este punto de partida, decir que para las personas que trabajamos en equipos de seguridad ha sido un reto profesional enorme. Nosotros nos preparamos permanentemente para gestionar crisis. Dentro de las competencias del área de seguridad de MAPFRE, está la gestión de crisis, para las que nos preparamos y ensayamos. Trabajamos cada año en planes de continuidad de negocio y contingencia para estar preparados cuando estas situaciones surgen.

Por ello esta crisis ha dado a los profesionales de seguridad la oportunidad de mostrar su aporte de valor a la compañía, evidenciar para que servían todas esas horas de entrenamiento, recursos económicos y personal dedicado. MAPFRE ha sido capaz de mantener el servicio en todo momento y lugar en todos los países donde opera. Hemos sido capaces de conseguir los objetivos que se nos marcaron desde el minuto cero en que irrumpió esta crisis. Primero, y antes de nada, protegiendo a nuestros empleados del mejor modo y manera posible y también a nuestros colaboradores, proveedores y a nuestros los clientes. En segundo lugar, garantizando la continuidad del negocio, es decir, el servicio a nuestros clientes y en tercero, apoyando a la sociedad.

Estos tres objetivos han sido alcanzados con un alto grado de cumplimiento y satisfacción, lo que genera en los profesionales de seguridad que hemos contribuido a ello, la legítima e íntima satisfacción del deber cumplido por haber estado a la altura de tan desafiante reto.

Habéis superado el reto con creces y se debe, en gran medida, al trabajo de preparación que mencionas. Este tipo de crisis también ofrecen una oportunidad para aprender. Desde el punto de vista de ciberseguridad, ¿qué lecciones aprendidas de toda esta experiencia destacarías?

Han sido varias las lecciones aprendidas. Desde el punto de vista de seguridad, lo primero que hemos hecho es ponernos a trabajar en la contingencia de la contingencia dada la prolongación de la crisis cuya duración jamás habríamos pensado.

Este hecho nos ha vuelto a recordar alguno de los principios básicos de la gestión de crisis, como el de que los cisnes negros existen y los escenarios reales son peores de los que puedes imaginar en el planeamiento.

El despliegue de este a oeste de la pandemia, desde China, Filipinas, Italia, España, América, etc. nos dio el tiempo suficiente para ir asimilando las lecciones aprendidas en la respuesta a la crisis en los escenarios donde primero se presentó y obtener sinergias. La realidad y visión global de MAPFRE ha sido catalizador de nuestra eficiencia para anticiparnos en aquellos territorios donde tenemos nuestras sedes, activando la gestión de crisis en las distintas geografías, incluso semanas antes de que los gobiernos reconocieran esta situación.

Más lecciones aprendidas: la necesidad de independizar el acceso del dispositivo de la ubicación física del usuario y que la filosofía *zero trust* o el concepto de malla de seguridad han venido para quedarse. Hemos implantado el doble factor de autenticación, —vinculado únicamente a determinados usuarios, a determinados entornos críticos antes de la pandemia— a todos los usuarios de MAPFRE en todo el mundo. Lo imprescindible de dotarnos de un modelo de seguridad homogénea como el que hemos mencionado o la necesidad de estar imbricado de forma intensa y permanente con las áreas de negocio antes y durante la crisis para poder darles el servicio que ellas demandan.

Desde el punto de vista de la evolución del mapa de riesgos de los últimos años, ¿qué vulnerabilidades y amenazas destacarías?

Llevamos años hablando del incremento de las amenazas, del crecimiento de los ataques de *ransomware* o de los de denegación de servicio, de la proliferación de campañas de *phishing*... Han aumentado tanto el volumen como la sofisticación de las amenazas.

El uso intensivo de la tecnología por parte de todas las empresas, con independencia de su tamaño, nos hace cada vez más dependientes de nuestros sistemas y datos y, por tanto, vulnerables en caso de ataques.

Frente a etapas anteriores en que las entidades financieras eran los principales objetivos, ahora en tanto en cuanto los delincuentes son capaces de denegar el servicio, robar el acceso a los datos o poner en riesgo la reputación, y extorsionarnos con ello, todos somos posibles objetivos de estos ataques. Este aumento del número de posibles objetivos ha producido un incremento del mercado para los ciberdelincuentes, que ha favorecido la escalabilidad del negocio de la ciberdelincuencia y la creación de grandes conglomerados que se dedican de forma intensiva a ella.

Además, hay un elemento que también ha actuado como catalizador del incremento de amenazas, que es la disminución del riesgo asociado. Ahora estos ataques pueden cometerse desde sitios lejanos y desconocidos, con herramientas que antes no existían como las redes de *botnets*, que permiten utilizar equipos para el fraude sin que sus usuarios lo sepan. La aparición de las criptomonedas que contribuyen a la opacidad de los flujos de capital obtenidos con actividades delictivas como la extorsión, robo, venta de datos, etc. favorecen igualmente la monetización rápida y segura de sus actividades delictivas.

Por último, el propio proceso de transformación digital de las compañías está generando una mayor dependencia y uso de los activos digitales. El número de dispositivos conectados no para de crecer, lo que unido a que con la pandemia y la generalización del teletrabajo las compañías han aumentado su superficie de exposición, ha creado la tormenta perfecta. El aumento de las amenazas está alcanzando ratios nunca vistos.

Las regulaciones en materia de ciberseguridad que se aplican en los países donde operáis, ¿las consideras adecuadas para proteger a las organizaciones como la vuestra?

La regulación es necesaria para que los estados y los gobiernos sean capaces de crear un entorno seguro, donde los datos de los ciudadanos estén protegidos frente a un riesgo que se ha incrementado en los últimos tiempos.

Abogaría por un marco regulatorio homogéneo, con reglas claras y con un adecuado equilibrio para no caer en la hiperregulación. Con entornos similares para todos, que favorezcan la libre competencia, por otra parte, esencia del progreso de nuestra sociedad.

> Se ha producido un incremento del mercado para los ciberdelincuentes que ha favorecido la escalabilidad del negocio de la ciberdelincuencia y la creación de grandes conglomerados que se dedican de forma intensiva a ella

El número de normas y leyes que existen en los países donde MAPFRE desarrolla su actividad es enorme, muchas cuentan con principios muy similares, pero con matices y cuestiones propios que obligan a unos esfuerzos de adaptación importantes.

La relación de colaboración entre MAPFRE y GMV se ha forjado durante muchos años. ¿Qué destacarías de este trabajo conjunto?

La relación entre MAPFRE y GMV se remonta a quince años atrás, con un nivel de colaboración creciente entre las compañías.

En MAPFRE buscamos relaciones basadas en la confiabilidad y el largo plazo, puesto que los entornos de seguridad son volátiles, con necesidades exigentes de respuesta a crisis. GMV ha demostrado en estos años ser una compañía confiable y con enorme conocimiento del mercado de la ciberseguridad y la tecnología de vanguardia.

Hemos encontrado su apoyo y la respuesta que hemos necesitado en los momentos de crisis, aportando su flexibilidad para adaptarse a MAPFRE y ayudarnos en el desarrollo y en la creación del camino por el cual transitamos, un camino que necesitamos escribir junto a socios que sean capaces de alumbrarnos. A su vez, GMV nos ha aportado algo que valoramos enormemente: su enorme conocimiento y experiencia.

Sólo puedo decir que estamos enormemente agradecidos al apoyo que hemos recibido de GMV todos estos años.

GMV se incorpora de manera oficial y plena a la fase inicial del programa NGWS/FCAS

La modificación contractual que permite a la industria española integrarse plenamente en las actividades de la Fase 1A de demostradores del proyecto NGWS/FCAS faculta la firma del correspondiente contrato con Airbus D&S GmbH, líder del Pilar Tecnológico de Operadores Remotos

El pasado mes de diciembre y gracias al excelente trabajo realizado por el Ministerio de Defensa español, la Direction Générale de l'Armament (DGA), en nombre de los gobiernos de España, Alemania y Francia, formalizó la modificación contractual que permitía a la industria española integrarse plenamente en las actividades de la Fase 1A de demostradores del proyecto NGWS/FCAS, que fue lanzada inicialmente por Francia y Alemania a principios de 2020.

Esta modificación contractual ha permitido la firma del correspondiente contrato con Airbus D&S GmbH (líder del Pilar Tecnológico de Operadores Remotos), también en diciembre, que da entrada a GMV, a través de la UTE SATNUS, en la Fase 1A de dicho pilar tecnológico. Este pilar se centra en el desarrollo de nuevas tecnologías y evaluación de nuevos conceptos —de manera coordinada con el nuevo avión tripulado de combate del NGWS/FCAS— basados en un conjunto de vehículos no tripulados.

El contrato correspondiente a esta fase cubre las actividades que se realizarán durante los primeros 18 meses y que están encaminadas al desarrollo de diversos demostradores y tareas de maduración tecnológica que permitan iniciar los primeros vuelos previsiblemente en 2026.

GMV aportará el conocimiento adquirido tras una larga trayectoria de actividad en proyectos internacionales de cooperación industrial. Este conocimiento se asienta en cuatro pilares: la contratación directa con agencias europeas y la OTAN, la venta de productos en el dominio JISR, la participación activa en programas de I+D y el espíritu cooperante de GMV, siempre abierto colaborar tanto con el resto de la industria como con los principales centros tecnológicos de investigación.

La participación de GMV se centra en tecnologías en las que la compañía ha desarrollado una intensa actividad en los últimos años, logrando alcanzar un notable reconocimiento en sectores tales como navegación, aviónica, sistemas autónomos e inteligencia artificial, entre otros.

El programa FCAS plantea el desarrollo de un «sistema de sistemas», que integra tanto plataformas aéreas tripuladas como no tripuladas. FCAS es uno de los mayores proyectos europeos en el ámbito de la defensa.

En paralelo, y también dentro del consorcio SATNUS, GMV trabaja en la preparación de la oferta para las fases 1B y 2, que darán continuidad al proyecto.

Nueva versión del sistema de monitorización ADS-B para ENAIRE

GMV ha entregado a ENAIRE una nueva versión del sistema APRESTA para la monitorización de prestaciones del servicio de vigilancia ADS-B en España, en el marco del contrato que este organismo adjudicó a GMV en 2019 para el desarrollo y mantenimiento de dicho sistema.

El sistema APRESTA permite la recogida y procesado en tiempo real de los flujos de datos en formato ASTERIX (*All Purpose Structured Eurocontrol Surveillance Information Exchange*), generados por múltiples estaciones ADS-B. También permite la generación periódica de informes de prestaciones que permiten verificar que el servicio de vigilancia ADS-B prestado en un determinado volumen de espacio aéreo cumple con los estándares ADS-B aplicables (ED-129B).

Otra funcionalidad destacada del sistema APRESTA, basada en el producto ***GNASSURE*** de GMV, es que permite detectar y localizar áreas donde las prestaciones GNSS se han degradado debido a la presencia de interferencias (RFI) generadas, de manera intencionada o no, desde algún sistema o dispositivo situado en el terreno que sobrevuelan las aeronaves afectadas.

Los eventos detectados sobre degradación de prestaciones GNSS son reportados igualmente por el sistema APRESTA en informes generados periódicamente. Además de la generación periódica de informes, el sistema APRESTA dispone de un servicio de alertas por el cual notifica a los usuarios registrados de cualquier desviación de las prestaciones ADS-B calculadas respecto a los valores requeridos, o de la detección de problemas GNSS. Finalmente, el sistema APRESTA incluye un interfaz web que permite el acceso simultáneo de múltiples usuarios para, entre otras posibilidades, la consulta del estado del sistema, la descarga de informes periódicos o la generación de informes específicos.

El sistema APRESTA ha sido desarrollado en estrecha colaboración con ENAIRE, cuyo conocimiento experto sobre el funcionamiento del sistema ADS-B en su operativa real ha permitido diseñar los algoritmos de procesamiento adecuados para dicho entorno.

Predicción de prestaciones de servicios GNSS para uso en aplicaciones de navegación y vigilancia aeronáutica

Se han cumplido los primeros seis meses de un contrato de tres años de duración que EUROCONTROL adjudicó en 2020 a GMV para la prestación del servicio de predicción de indisponibilidades GPS/RAIM y la generación de propuesta de NOTAMs (*Notices to Airmen*) para aeródromos que disponen de procedimientos de vuelo instrumentales basados en GNSS.

Dicho servicio, conocido como AUGUR y que EUROCONTROL pone de manera gratuita a disposición de pilotos, usuarios del espacio aéreo (ej. aerolíneas) y proveedores de servicios de navegación aérea (ANSPs), consta de dos elementos principales.

En primer lugar, de un sitio web (*https://augur.eurocontrol.int/help/*), que permite a cualquier usuario conocer las indisponibilidades del servicio GPS/RAIM previstas durante los próximos tres días en cualquier aeropuerto situado en los estados miembros de ECAC y MEDA. En segundo lugar, de un interfaz para el envío automático de las propuestas de NOTAMs asociadas a dichas indisponibilidades. Estas propuestas de NOTAMs son enviadas a EAD (*European AIS database*) para su posterior publicación en el NOF (*NOTAM Office*) de cada país con el fin de que puedan ser consultadas por los usuarios aeronáuticos.

Las regiones ECAC y MEDA engloban 44 países europeos y 12 países del norte de África y Oriente medio, respectivamente, y en conjunto representan a más de mil aeropuertos repartidos por todo el mundo, incluyendo territorios de ultramar de varios países europeos.

El servicio prestado por GMV incluye el *hosting* del sistema que presta los servicios descritos, su mantenimiento, así como un servicio de *help-desk* a los usuarios de AUGUR.

El sistema utilizado en este servicio está basado en el producto ***GNASSURE*** de GMV, que permite la predicción de prestaciones de servicios GNSS para su uso en aplicaciones de navegación y vigilancia (p.ej. ADS-B) en aviación.

Unidades de élite españolas reciben las primeras unidades del RPAS Seeker

A finales de 2020, el Ejército de Tierra y la Armada recibieron las primeras unidades del RPAS Seeker, el sistema aéreo no tripulado que permitirá reforzar las capacidades de inteligencia, vigilancia y reconocimiento de la Brigada «Almogávares» VI de Paracaidistas del Ejército de Tierra y de la Brigada de Infantería de Marina del Tercio de Armada, dos unidades que gozan de prestigio como fuerzas de élite a nivel internacional.

El RPAS Seeker constituye uno de los sistemas más eficaces en su segmento con una autonomía de 90 minutos, un alcance de 15 km y un peso de 3,5 kg. El diseño de la aeronave y sus sistemas se han llevado a cabo en España por GMV y Aurea Avionics. Su fabricación se ha mantenido en territorio nacional, lo que ha sido clave para mitigar los efectos de la ruptura de las cadenas de suministro producida a principios y mediados de año.

La fabricación, los ensayos en vuelo y la transferencia de las aeronaves se han realizado en los plazos establecidos en la planificación inicial del proyecto. Pese a las dificultades motivadas por la pandemia de la COVID-19, se han cumplido sin incidencias las fechas de entrega acordadas, gracias a un cambio en las dinámicas de trabajo y reorganización de las actividades por parte del personal de ambas firmas y del Ministerio de Defensa.

El RPAS Seeker proporcionará a ambas unidades vídeo en tiempo real en espectros visible y térmico, aumentado con metadatos que son explotables *in situ* por el operador y en remoto por estaciones «centrales» de mando y control. Esto se debe a la nueva arquitectura de las estaciones terrestres, que han sido digitalizadas por completo para permitir la integración del RPAS Seeker con los centros de mando con estándares de la OTAN, por lo que cualquier fuerza aliada puede integrar de manera directa la aeronave en su flota y centros de mando, algo que añade versatilidad y facilita operatividad conjunta entre tropas y sistemas. De este modo, se combina un producto de ADN 100 % nacional y una fuerte proyección internacional, que le permite formar parte tanto del proyecto de modernización de las Fuerzas Armadas españolas como integrarse plenamente en la creciente cooperación y colaboración de las industrias de defensa a nivel europeo.

El sistema ha sido financiado por la Subdirección General de Planificación, Tecnología e Innovación de la DGAM dentro del proyecto RAPAZ.

GMV mejora la capacidad de autonomía de los RPAS

Finalizada la fase de definición, recientemente ha dado comienzo una nueva fase de SAFETERM, proyecto de la Agencia Europea de Defensa (EDA) y que GMV desarrolla en colaboración con AERTEC.

SAFETERM tiene por objeto mejorar los sistemas y procedimientos actuales de terminación de vuelo de media altitud y larga duración (MALE) y de grandes sistemas tácticos de aeronaves pilotadas a distancia (RPAS). El sistema SAFETERM proporcionará a los RPAS un mayor nivel de autonomía para situaciones de emergencia, en particular las que implican la pérdida/degradación del enlace de mando y control, así como otros fallos.

Más concretamente, SAFETERM permite una terminación segura del vuelo en caso de fallo tanto de la autonomía como de la capacidad de control del piloto a distancia, mediante el establecimiento de áreas alternativas de terminación de vuelo para evitar daños personales o patrimoniales.

Durante esta fase el equipo del proyecto mejorará el demostrador SAFETERM utilizando hardware y software de aviónica real. Para el diseño se seleccionará una plataforma de procesador certificable, y el software se dividirá en particiones en un sistema operativo en tiempo real (SOTR) certificable. Aunque no se prevén actividades reales de certificación para el desarrollo, los procedimientos de certificación se utilizarán como guía para la formación de aprendizaje automático y la extracción de parámetros de verificación. El principal aspecto del aseguramiento se centrará en el desarrollo y la aceptación del algoritmo de clasificación.

Para la recopilación de los datos del vuelo, está prevista una campaña de vuelo con el avión TARSIS-75 de AERTEC. El objetivo de estos vuelos será grabar vídeos de diferentes características del terreno a diferentes altitudes y en diferentes condiciones de iluminación. Cada vídeo grabado se dividirá en dos conjuntos de imágenes que se utilizarán para entrenamiento y validación por separado.

Otro aspecto relevante del proyecto está relacionado con las actividades de apoyo a la certificación y normalización. Actualmente, GMV es miembro del Comité Internacional Conjunto de Inteligencia Artificial en la Aviación SAE G34 / EUROCAE WG 114, que promueve el cumplimiento de la certificación de la inteligencia artificial (IA) dentro de los sistemas aeronáuticos críticos para la seguridad.

Futuras operaciones civiles y militares con vehículos aéreos no tripulados

El 4 de febrero GMV organizó el seminario web «Future Civil and Military Operations using Unmanned Aerial Vehicles», presentado por Carlos Molina, jefe de proyecto en la división de Sistemas de Aviónica de GMV.

En este seminario se abordaron los avances más relevantes que se prevén en relación al uso de vehículos aéreos no tripulados en el ámbito civil, entre los que destacaron conceptos como U-Space o *Urban Air Mobility* (UAM). Carlos Molina repasó diferentes aplicaciones civiles en los que los sistemas aéreos no tripulados están siendo utilizados en la actualidad, así como futuros casos de uso de estos sistemas, como por ejemplo el uso de estos vehículos como taxis aéreos. También se presentaron distintos servicios U-Space, desarrollados por GMV e incluidos dentro de la suite ***Dronelocus®***, que se integraron en el demostrador U-Space del proyecto DOMUS, coordinado por ENAIRE.

En esta presentación también se destacaron los avances relativos a los sistemas aéreos no tripulados en el ámbito militar, donde este tipo de vehículos jugará un papel fundamental en los futuros programas de defensa.

Finalmente, Carlos Molina repasó algunas de las contribuciones más relevantes de GMV en relación a UAS en distintos programas de defensa, como son el suministro de varios sistemas aéreos no tripulados Seeker al Ministerio de Defensa, así como la participación de GMV en el consorcio SATNUS, coordinador nacional del Pilar Tecnológico de Operadores Remotos en el programa NGWS/FCAS.

GMV investiga la integración de la IA en sistemas GNC aeronáuticos

La Agencia Europea de Defensa (EDA) adjudica a GMV el proyecto AI-GNCAir cuya finalidad es investigar la nueva tecnología de guiado, navegación y control para su aplicación en sistemas aéreos

En el sector aeronáutico, y más concretamente en las aplicaciones de guiado, navegación y control (GNC), la gestión de datos de los sensores se debe procesar de manera que permita asegurar un alto nivel de integridad, detectando e impidiendo la propagación de medidas incorrectas o injerencias externas para mejorar la precisión, integridad y disponibilidad de las soluciones.

Las tecnologías IA pueden ser de gran utilidad en el cumplimiento de estos objetivos, ya que reconocen las interferencias en las señales y las lecturas incorrectas de sensores o predicen los datos que podrían faltar como consecuencia de dichas interferencias y lecturas incorrectas. En consecuencia, se busca la mejora de los sistemas GNC no solo para lograr un mayor rendimiento, sino también para la reconfiguración dinámica de los sensores mediante la determinación de la calidad de los datos y la detección de un rendimiento deficiente de los sensores.

En este contexto, la Agencia Europea de Defensa (EDA) ha adjudicado a GMV el proyecto AI-GNCAir cuya finalidad es investigar la nueva tecnología de guiado, navegación y control para su aplicación en sistemas aéreos. Esta iniciativa forma parte de la agenda de investigación estratégica de la EDA dentro del CapTech GNC, que estudia la forma de integrar la tecnología de la inteligencia artificial en los sistemas GNC y las hojas de ruta necesarias para reducir las brechas tecnológicas asociadas en la UE.

AI-GNCAir, liderado por GMV y desarrollado en colaboración con el Centro de Investigación en Procesado de la Información y Telecomunicaciones de la Universidad Politécnica de Madrid (UPM-IPTC), se centrará en la fusión inteligente de datos para localización absoluta y relativa mediante la aplicación de las tecnologías de IA en los sistemas GNC de aviónica.

AI-GNCAir investigará la tecnología más avanzada en el uso de la fusión inteligente de datos para la autolocalización de vehículos aéreos. El proyecto tiene como objetivo recomendar una arquitectura GNC genérica para la utilización segura de algoritmos basados en IA en el ámbito aeronáutico. En una segunda fase del proyecto, se simulará un caso práctico para comparar las prestaciones de los nuevos algoritmos frente a las técnicas tradicionales de fusión de datos.

GMV consolida su liderazgo en la gestión de tráfico espacial

GMV elegida por la Comisión Europea para dirigir un proyecto de coordinación y apoyo (CSA) para la presentación de propuestas de desarrollo futuro de una capacidad europea en el área de gestión de tráfico espacial (STM)

GMV, líder europeo en los programas SSA (*Space Situational Awareness*) y SST (*Space Surveillance and Tracking*), ha sido elegida por la Comisión Europea para dirigir un proyecto de coordinación y apoyo (CSA) enmarcado en el programa H2020 para la presentación de propuestas de desarrollo futuro de una capacidad europea en el área de gestión de tráfico espacial (STM): EUSTM.

La actividad espacial se ha incrementado de manera exponencial en las últimas décadas. La aparición de nuevos actores públicos y privados, así como de nuevos conceptos, como pequeños satélites y grandes constelaciones, servicios de puesta en órbita de satélites, cohetes reutilizables, etc., plantean nuevos desafíos. Es probable que el número de objetos en órbita aumente de manera drástica y, por ello, va a ser necesario desarrollar capacidades

para conseguir su gestión eficiente. También es cada vez más necesario contar con un marco regulador y un marco jurídico que se fundamenten en los avances tecnológicos y contribuyan a promover y garantizar la seguridad, la sostenibilidad y la estabilidad deseadas de las operaciones espaciales. Estos marcos son los que se conocen, de manera general, como gestión de tráfico espacial (STM), mientras que la tecnología que lo sustenta se denomina conocimiento de la situación en el espacio (SSA) o vigilancia y seguimiento espacial (SST).

Europa se beneficia en gran medida de la política abierta del gobierno federal de EE. UU. en términos de acceso datos y servicios SSA/SST por medio de acuerdos de intercambio de datos SSA. Sin embargo, con el fin de asegurar su soberanía, autonomía y liderazgo en este ámbito y reducir esta dependencia, la Comisión Europa ha comenzado a trabajar en una capacidad SSA/SST independiente.

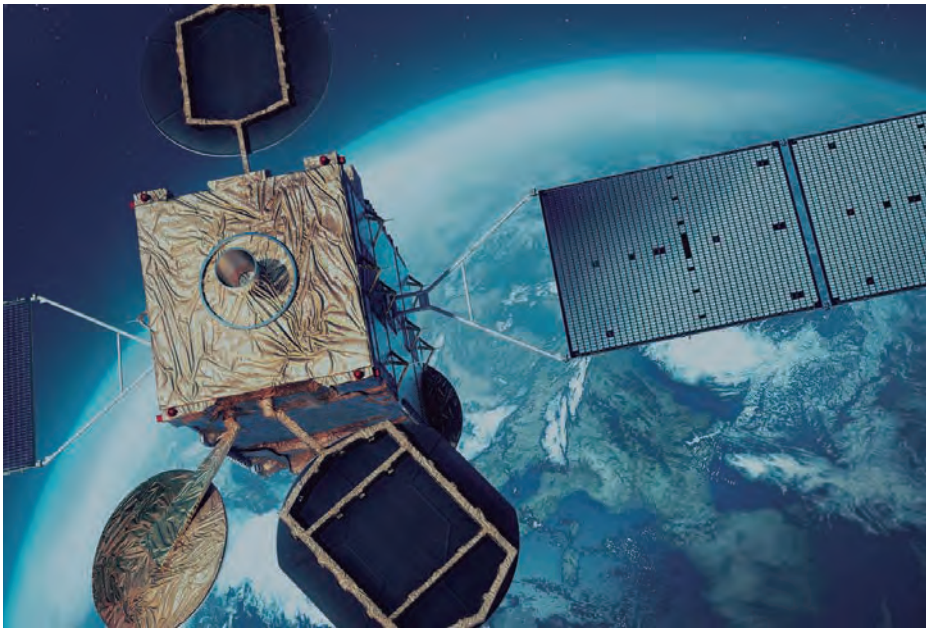
El objetivo de EUSTM es fortalecer el sector espacial público y privado, impulsar una industria espacial innovadora, competitiva y rentable y contribuir al crecimiento de una comunidad investigadora que desarrolle y ponga en marcha infraestructuras espaciales. EUSTM implantará una plataforma colaborativa para promover el intercambio de información entre los miembros del equipo y también con actores relevantes externos al mismo. El objetivo de esta plataforma es crear una comunidad activa de interés que constituya una fuente interminable de información STM para la Comisión Europea.

El consorcio EUSTM, encabezado por GMV, está formado por las 18 siguientes empresas e instituciones europeas: Weber-Steinhaus and Smith (Alemania); Europaisches Institut fur Weltraumpolitik (Austria); Spacetec Partners SRL y Qinetiq Space NV (Bélgica); GomSpace (Dinamarca); Centro de Satélites de la Unión Europea, ENAIRE y Payload Aerospace, SL (España); Iceye Oy (Finlandia); Eutelsat SA, PriceWaterhouseCoopers Advisory SAS, Office National d'Estudes et de Recherches Aerospatiales, Safran y Université Paris-Saclay (Francia); AVIO SPA (Italia); y Universitaet Bern, Clearspace SA y Sceye SA (Suiza).

Este proyecto está cofinanciado por el programa de investigación e innovación Horizon 2020 de la Unión Europea en el marco del acuerdo de subvención n.º 101004319

Este artículo refleja la opinión del autor y no necesariamente la opinión de la Comisión Europea o de la Agencia Ejecutiva de Investigación de la UE

GMV suministra el segmento terreno de los nuevos satélites de la flota de Eutelsat



Eutelsat ha vuelto a confiar a GMV la implementación de su centro de control conocido como NEO, versión para EUTELSAT del producto de GMV, ***Hifly***®, así como del sistema de dinámica de vuelo FOCUS basado en la cartera de productos ***Focussuite*** para sus próximas tres nuevas misiones: Konnect VHTS y Hotbird 13F & 13G.

Konnect VHTS es un satélite perteneciente a la familia Spacebus Neo construido por Thales Alenia Space y que forma parte de una nueva generación de sistemas VHTS (*Very High Throughput Satellite*). Mientras que Hotbird 13F y 13G son dos nuevos satélites de la plataforma Eurostar Neo, construidos por Airbus Defence and Space con el objetivo de sustituir anteriores misiones de la órbita Hotbird.

Eutelsat, uno de los clientes de referencia de GMV, cuenta con sistemas desarrollados por GMV para el control de su flota de satélites al completo, entre los que destacan los citados sistemas de control de satélites multiplataforma y multisatélite NEO y de dinámica orbital FOCUS, así como nuevas herramientas de gestión de carga de pago de última generación.

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 también incrementar el número de desarrollos y actividades realizadas para Eutelsat.

Los sistemas proporcionados por GMV se harán cargo de la gestión de las operaciones en tierra de estos tres nuevos satélites cuyas fases operacionales enfocadas a labores de verificación y validación en tierra (SVT) están previstas durante los primeros meses de 2021.

Lanzamiento del satélite Türksat 5A

Superadas con éxito las pruebas de verificación y validación en tierra (SVT), el día 8 de enero, tuvo lugar con éxito el lanzamiento del satélite Türksat 5A desde el Space Launch Complex 40 (SLC-40) de la estación de Cabo Cañaveral.

GMV ha sido la encargada de suministrar el software instalado en el centro de control de la misión (SCC) —***Hifly***©, *Flight dynamics system* y ***Smart rings***— dando soporte a Airbus DS (fabricante) y a Türksat (como contratista principal) durante la fase de pruebas SVT y de lanzamiento.

El satélite Türksat 5A se basa en la reciente versión *Electric Orbit Raising* (EOR, elevación eléctrica a órbita) de Eurostar E3000, la plataforma altamente fiable y a un coste razonable de Airbus, que utiliza propulsión eléctrica para su elevación a órbita y para mantener su posición. EOR tardará 4 meses en conseguir la elevación a la órbita final.

Türksat 5A es un satélite de difusión que operará en transpondedores de banda Ku en la posición orbital geoestacionaria de 31 grados de longitud Este y que dará cobertura a Turquía, Oriente Medio, Europa, África del Norte y África del Sur. Tiene una masa de lanzamiento de 3.500 kg y su potencia eléctrica alcanzará los 12 kW. Tiene una vida útil en órbita prevista de 15 años.

Validación del servicio de autenticación de Galileo

Galileo inicia la fase de validación de la señal en el espacio del servicio de autenticación (OSNMA), un servicio que junto con el servicio de alta precisión es uno de los principales valores añadidos que aporta la constelación Galileo

Recientemente ha tenido lugar un importante hito en el marco de los sistemas globales de navegación por satélite (GNSS), así como para la comunidad mundial de GNSS. En noviembre, Galileo inició la fase de validación de la señal en el espacio del servicio de autenticación (OSNMA). El Centro Europeo de Servicios de GNSS (GSC) es el responsable actual de generar el mensaje de autenticación y de enviarlo al segmento de misión en tierra de Galileo. Este servicio de autenticación es, junto con el servicio de alta precisión, uno de los principales valores añadidos que aporta la constelación Galileo.

El GSC forma parte de la infraestructura del programa europeo de navegación Galileo. Su función principal es actuar como interfaz única con los usuarios EGNSS y contribuir a la prestación de servicios de OSNMA y de alta precisión. El centro también está concebido como un centro experto para facilitar el intercambio de conocimientos, ayudar a los desarrolladores, dar a conocer el GNSS y brindar apoyo a la prestación de servicios de valor añadido.

El GSC, situado en Madrid, está gestionado por la Agencia Europea de GNSS (GSA) con la colaboración de España, que proporciona al programa Galileo la infraestructura y las instalaciones necesarias para albergar el centro. En 2014, un consorcio liderado por GMV junto con Indra se adjudicó el contrato marco para el suministro de la infraestructura del GSC, manteniendo esta responsabilidad desde entonces. Desde ese año, GMV también lidera para la Comisión Europea el proyecto AALECS de experimentación de los servicios de alta precisión y autenticación a través de los servicios comerciales, que puso en marcha los primeros prototipos de OSNMA.

La nueva versión del GSC, que da apoyo a la fase de ensayos de OSNMA, ya está operativa. OSNMA garantiza que los datos de navegación recibidos proceden de un satélite Galileo y que no están falseados. Esta capa de verificación proporciona una fuerte protección a la constelación Galileo. Se trata de un gran logro para el GNSS europeo; es la primera señal de una constelación de satélites de navegación que provee este servicio en todo el mundo, lo que convierte a Galileo en el sistema de GNSS más sólido y seguro. Esta nueva versión del GSC permite al Programa Galileo preparar la futura fase de observación pública de OSNMA.

El consorcio de infraestructura del GSC ha desempeñado un papel importante en este gran éxito, poniendo de relieve la labor de GMV y reafirmando su posición como socio fiable. Durante la fase de implantación, el consorcio ha estado trabajando estrechamente con la GSA y con otras partes interesadas, como la Comisión Europea, para desarrollar el GSC, mejorar los servicios de Galileo y situar a Europa a la cabeza mundial en el campo de la navegación segura y sólida.

GMV ahonda en las sinergias entre física fundamental y sistemas PNT

Recientemente ha finalizado Positrino, un proyecto de la Agencia Espacial Europea (ESA) desarrollado por un consorcio liderado por GMV, cuyo objetivo ha sido estudiar la viabilidad de un sistema de posicionamiento, navegación y tiempo (*Positioning, Navigation and Timing* o PNT) basado en neutrinos.

Los neutrinos son una partículas fundamentales del modelo estándar de la física de partículas que interaccionan muy débilmente con la materia y viajan prácticamente a la velocidad de la luz por lo que pueden acceder a entornos en los que las señales GNSS están bloqueadas como por ejemplo, entornos subterráneos o submarinos. De ahí que un sistema PNT basado en estas partículas podría resultar útil por ejemplo para la navegación de submarinos, naves espaciales o para aplicaciones de minería.

En el proyecto, de un año de duración, también se ha propuesto un diseño a alto nivel de un sistema basado en fuentes artificiales de neutrinos isotrópicas y en detectores de neutrinos miniaturizados y se han realizado distintas simulaciones de física de partículas y de prestaciones PNT para estudiar su viabilidad.

Positrino ha demostrado que, teniendo en cuenta las tecnologías actuales de generación y detección de neutrinos así como los avances que se están dando en tecnologías de estas partículas, un sistema de estas características es viable a corto-medio plazo.

En los próximos meses está previsto que la ESA contrate nuevas actividades técnicas para consolidar el diseño a alto nivel de un sistema de estas características, así como para realizar pruebas de concepto que allanen el camino para su posible desarrollo operacional una vez que los estudios de viabilidad técnica y económica hayan sido favorables.

GMV está intensamente involucrada en proyectos de la ESA (liderados por Galileo Science Office en ESAC, Madrid) que explotan sinergias entre la física fundamental y tecnologías PNT. En esta línea, GMV también está liderando el consorcio del proyecto Lifeline, iniciado en noviembre de 2020, para un estudio de viabilidad y diseño a alto nivel de un sistema de posicionamiento relativista, es decir, de un sistema PNT que incorpore de forma natural la teoría de la relatividad de Einstein.

Renovación del contrato marco para la prestación del servicio de vigilancia de fronteras de Copernicus

Los objetivos del servicio son reducir el número de inmigrantes ilegales que entran en la UE sin ser detectados, reducir la pérdida de vidas humanas en el mar y aumentar la seguridad interna de la Unión Europea en su conjunto contribuyendo a la prevención de la delincuencia transfronteriza

GMV forma parte del consorcio que ha resultado recientemente adjudicatario del contrato marco convocado por el Centro de Satélites de la Unión Europea para continuar con la prestación del servicio de vigilancia de fronteras Copernicus. GMV lleva trabajando en este servicio desde el inicio de las operaciones en 2015.

Los objetivos del servicio son reducir el número de inmigrantes ilegales que entran en la UE sin ser detectados, reducir la pérdida de vidas humanas en el mar y aumentar la seguridad interna de la Unión Europea en su conjunto contribuyendo a la prevención de la delincuencia transfronteriza. El servicio contribuye al marco de intercambio de información sobre la vigilancia de las fronteras exteriores de la UE (EUROSUR/FRONTEX) y proporciona datos casi en tiempo real sobre lo que ocurre en tierra alrededor de las fronteras de la UE.

Los productos desarrollados consisten en mapas de referencia con una amplia gama de características observables extraídas mediante observación terrestre y datos de código abierto y proporcionan un fondo de contexto geográfico y de representación de las superficies de los países, lo que incluye la hidrografía, la topografía, la cubierta terrestre, la infraestructura y las actividades de la población. En función de las necesidades y peticiones de los usuarios, se obtienen imágenes de retorno humanitario voluntario (RHV) según sea necesario (fecha y hora de obtención, cobertura de nubes y resolución, etc.) que se utilizan para extraer información actualizada. Los mapas se generan a escalas entre muy grandes y grandes (1:5.000 - 1:100.000).

Los productos son proporcionados en forma de datos vectoriales y cartográficos (planos), representados dentro de una única hoja de mapa en formato vertical o apaisado y en diferentes tamaños de página (de A0 a A2).

GMV presenta su solución sobre la detección de daños de plagas en bosques

El pasado 21 y 22 de enero, GMV participó en el seminario titulado «Daños del escarabajo de la corteza en el dominio SCERIN: detección, monitoreo y dinámica asociada al cambio de cobertura terrestre», organizado por la Red de Información Regional de Europa Meridional, Central y Oriental (SCERIN) para la Observación Mundial de la Dinámica de los Bosques y el Uso de la Tierra (GOFC-GOLD).

El encuentro giró en torno a la repercusión de los brotes de escarabajo de la corteza sobre los bosques de Europa Central y Oriental. Esta especie de insecto ataca a la corteza de los árboles debilitándolos hasta llegar a provocar su muerte. Cuando la población de este coleóptero alcanza el grado de plaga, puede producir la devastación de grandes extensiones forestales y provocar importantes pérdidas económicas y ambientales.

Ángel Fernández, Earth Observation Data Scientist de la división Remote Sensing & Geospatial Analytics de GMV, presentó el uso de datos de los satélites Sentinel-2 para la detección de los daños causados por este escarabajo de la corteza en bosques europeos. Fernández destacó el desarrollo y resultados del producto de daño biótico de GMV, una solución tecnológica que busca la detección, delimitación y estimación del daño causado por plagas en masas forestales a través de técnicas de *machine learning* y que ha sido desarrollada en el marco del proyecto MySustainableForest, liderado por GMV.

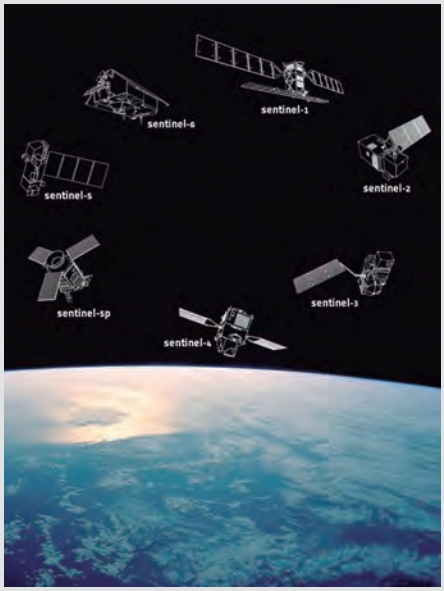
El estudio sobre los resultados del impacto de estas plagas se presentaron asimismo en el artículo científico «Monitoring Bark Beetle Forest Damage in Central Europe. A Remote Sensing Approach Validated with Field Data», publicado en octubre en la revista Remote Sensing y que ha sido elaborado por GMV en colaboración la Universidad Mendel en Brno (República Checa), también miembro del consorcio MySustainableForest.

GMV participante habitual en jornadas como representante clave del sector *downstream* espacial

Por su posición como actor clave en el sector *downstream* de las aplicaciones terrestres basadas en tecnología espacial, GMV ha sido invitada a participar en diversos *webinars* y eventos celebrados en Portugal.

En noviembre de 2020, dentro del «Encontro com a Ciência e Tecnologia» organizado por el sector institucional nacional a través del Ministerio de Ciencia, Tecnología y Educación Superior, Teresa Ferreira, directora de Espacio de GMV en Portugal, participó en una mesa redonda para hablar sobre el programa espacial propuesto por la Comisión Europea. Teresa puso de relieve el importante papel de GMV en el sector de la explotación terrestre de las tecnologías espaciales y ofreció, además, una perspectiva industrial nacional del programa y su importancia estratégica e impacto en la economía portuguesa.

Dentro del seminario centrado en aplicaciones marítimas, Filipe Brandão de GMV en Portugal presentó el caso de estudio titulado «Contaminación – detección y vigilancia de basura marina» y en el seminario dedicado a las aplicaciones terrestres, António Araújo, jefe de proyecto de GMV en Portugal, habló sobre las capacidades de GMV con la ponencia «Gestión de emergencias – Mapeado de riesgos y recuperación».



GMV explora la instalación de nuevo observatorio Copérnicus en el Ártico

La extraordinaria disminución del hielo marino en el Ártico abre nuevas oportunidades económicas: permite la navegación por nuevas rutas, el transporte de mercancías y el acceso a recursos naturales todavía sin explotar. Sin embargo, suscita una gran preocupación por las amenazas medioambientales y los problemas de seguridad que se derivan de la explotación intensiva de recursos naturales y las costas que lo rodean.

El riesgo de desastres en el mar, como los derrames de crudo o la proliferación de nuevas infraestructuras costeras podrían atentar contra la seguridad europea. El consenso de la UE sobre el mantenimiento de un enfoque de cooperación multilateral que garantice la estabilidad y las soluciones dialogadas en la región ha hecho crecer la concienciación social sobre el tema dentro de la UE.

En este contexto, acaba de iniciarse un nuevo proyecto en el marco del programa Horizonte 2020: el Observatorio Ártico Copernicus de apoyo al Servicio de Acciones Exterior (ARCOS). El objetivo de ARCOS, desarrollado por un consorcio, es diseñar e implantar un sistema de alerta rápida capaz de llevar a cabo una vigilancia continua de la región ártica y de proporcionar productos operativos en el ámbito de la seguridad. El sistema busca integrar fuentes de datos espaciales y no espaciales, así como productos temáticos de otros servicios ya operativos del Copernicus.

GMV participa en el consorcio encabezado por e-GEOS, junto con el Centro de Satélites de la UE, el Instituto Meteorológico de Finlandia, la Universidad Politécnica de Milán, el operador finlandés de constelaciones ICEYE SAR y la consultora danesa COWI.

Los productos de ARCOS darán respuesta a tres niveles de necesidades de información: primero, avisos automáticos de alarma rápida bajo ciertas condiciones; segundo, alertas establecidas por usuarios, basadas en indicadores requeridos por las aplicaciones específicas y tercero, productos de inteligencia geoespacial derivadas de los anteriores, que requieran análisis experto.

El proyecto se enfrenta a varios retos en el terreno del procesamiento de datos, desde la extensión del área bajo vigilancia a las condiciones extremas de luz y los ángulos de observación del satélite. Además, tiene previsto probar las más modernas tecnologías de inteligencia artificial para extracción automática de características y analítica.

Las aplicaciones de ARCOS en materia de seguridad comprenden ámbitos como la explotación de recursos marinos (acuicultura, pesca ilegal), transporte y comunicación seguros (conectividad, transporte marítimo autónomo, logística) y ordenación del espacio marítimo (protección de las costas, energías renovables, infraestructuras portuarias).

Transformación digital aplicada a la agricultura de precisión y la teledetección

Hoy en día estamos viviendo la transformación digital de la agricultura, que nos llevará a una agricultura más productiva y, a la vez, más eficiente y sostenible.

Primero fue la mecanización de muchas labores agrícolas gracias a las máquinas de vapor, después llegó la electricidad y los combustibles. La tercera revolución, llamada «revolución verde», vino con la incorporación de semillas mejoradas, fertilizantes y fitosanitarios a la que se unió el desarrollo espectacular de maquinaria pesada para todo tipo de tareas. Ahora la cuarta revolución se está produciendo con la incorporación de las nuevas tecnologías de la información y la comunicación, especialmente con herramientas como el big data y la inteligencia artificial.

Bajo el título genérico «Hacia la cuarta revolución agraria», Cajamar organizó durante enero varios seminarios en los que se abordaron en profundidad diferentes ámbitos de esta nueva revolución. En uno de ellos, GMV participó para hablar sobre sus capacidades con respecto a la transformación digital en el sector agro, concretamente en la agricultura de precisión y la teledetección.

Miguel Hormigo, director del Sector Industria de Secure e-Solutions de GMV, y Antonio Tabasco, responsable del área de Teledetección y Análisis Geoespacial de Espacio de GMV, presentaron las soluciones en las que está trabajando GMV dentro del concepto Smart Agro, como la inteligencia artificial para clasificar imágenes o la trazabilidad de activos para luego profundizar en el servicio avanzado de análisis de datos geoespaciales que apoya la toma de decisiones en agricultura (***Wineo***).

Comprobación de modelos para la verificación formal de sistemas espaciales

La ingeniería de sistemas basada en modelos (ISBM) es la práctica adoptada para dominar la creciente complejidad y heterogeneidad de los (sistemas de) sistemas actuales en fase de desarrollo. Integrada en un proceso de desarrollo basado en modelos, como el modelo en cascada, y con el apoyo de numerosos instrumentos, ISBM ofrece una solución completa que pretende derivar, posiblemente de forma (semi) automática, implantaciones a partir de especificaciones de alto nivel.

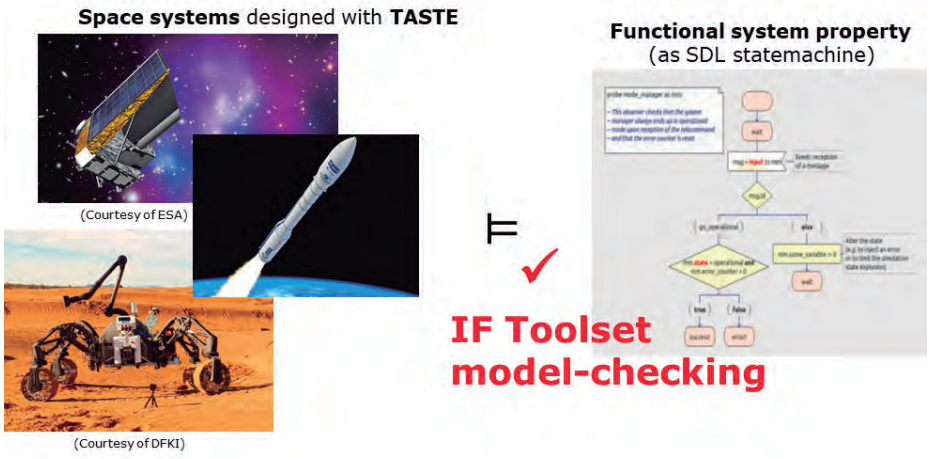
TASTE (*https://taste.tools/*), desarrollado por la Agencia Espacial Europea, es un instrumento pragmático de ISBM que reúne una serie de tecnologías que cubren un amplio espectro, desde el modelado de datos y comportamientos hasta la generación automática de aplicaciones binarias para sistemas incorporados.

Recientemente GMV ha empezado a trabajar en el proyecto MoC4Space, cuyo objetivo es introducir en el instrumento TASTE un planteamiento de comprobación de modelos que automatice la verificación de propiedades funcionales complejas para sistemas de software espacial incorporados.

La comprobación de modelos es una técnica de verificación formal que comprueba exhaustivamente si la propiedad deseada del sistema se satisface o no. La solución que se va a implantar en el proyecto se basa en el conjunto de instrumentos IF (*https://www-verimag.imag.fr/~async/IF/index.html*) como complemento de la comprobación de modelos. A continuación, los diseños de TASTE/SDL y las propiedades modeladas se traducen al lenguaje IF y se aplica la comprobación de modelos. Los resultados obtenidos se representan en el modelo TASTE, especialmente cuando se generan contraejemplos (comportamientos que invalidan la propiedad).

Durante el proyecto se abordarán varios retos, como el modelado de las propiedades del sistema (condiciones de parada, diagramas de secuencia de mensajes y observadores) en TASTE, la definición de la semántica de ejecución formal de TASTE, la transformación entre TASTE y los modelos IF y la integración sin fisuras del planteamiento dentro de la IGU de TASTE. Por último, el enfoque implantado se validará en dos casos de estudio espaciales representativos: un sistema integrado en vuelo y un sistema autónomo de exploración robótica espacial.

El proyecto MoC4Space está liderado por GMV y cuenta con la Universidad Jean Jaurès Toulouse II y el CNRS/VERIMAG como subcontratistas.



GMV desarrolla una metodología para la detección remota de basura marina

GMV ha desarrollado un enfoque novedoso basado en datos remotos para la detección de desechos marinos utilizando imágenes satelitales y técnicas de aprendizaje automático

GMV ha desarrollado un enfoque novedoso basado en datos remotos para la detección de desechos marinos utilizando imágenes satelitales proporcionadas por el satélite Sentinel-2, del programa europeo de observación de la Tierra (EO), Copernicus, y técnicas de aprendizaje automático (*machine learning*). Este método de procesado y análisis de datos de satélite de EO permite detectar posibles desechos marinos, clasificando y cuantificando la fracción de residuos presente con una resolución de imagen del tamaño de un píxel. Ya se han realizado las primeras investigaciones de detección e identificación de residuos plásticos, por ejemplo plásticos tipo PET, bajo este método que actualmente se encuentra en fase de desarrollado y validación en el marco de diferentes proyectos y áreas de estudio, entre los que cabe destacar los proyecto BEWATS, ATIN-BLUECO y PLESS.

GMV, en colaboración con la Universidad de Vigo y el Instituto de Ciencias Matemáticas (CSIC-UAM-UCM-UC3M), desarrolla el proyecto BEWATS. El objetivo es la detección, seguimiento y trazabilidad de los desechos visibles (macroplásticos y otros) que llegan a las playas y otras áreas costeras de Galicia (España), con el fin de buscar soluciones a ésta problemática y establecer estrategias de limpieza más eficientes utilizando nuevas fuentes de información. BEWATS está financiado por el Programa Pleamar de la Fundación Biodiversidad del Ministerio para la Transición Ecológica y el Reto Demográfico de España.

El proyecto Blue Economy (ATIN-BLUECO), liderado por GMV y financiado por la Agencia Espacial Europea (ESA), tiene como objetivo desarrollar y demostrar soluciones de datos impulsadas por tecnologías de observación de la Tierra que proporcionen información procesable sobre basura marina y vertidos de petróleo, entre otras aplicaciones, a los principales actores costeros. Este proyecto se centra en la zona geográfica del puerto de Vigo, en Galicia (España), Azores (Portugal) y en Argentina.

Por último, en febrero de 2021, GMV ha comenzado a trabajar como contratista principal en *Plastic-Less Society* (PLESS), proyecto financiado por la ESA y desarrollado en colaboración con el Research Centre of IST for Marine, Environment and Technology (Instituto Superior Técnico, Lisboa). En PLESS se hará un estudio para investigar la viabilidad técnica y económica de emplear las aplicaciones espaciales en apoyo a la reducción del impacto medioambiental de la basura plástica.

Además de estos proyectos, GMV también ha validado dicho enfoque en otras localizaciones de Europa, América del Sur y África, donde se disponen de datos abiertos (*open data*) sobre basura marina.

GMV presenta los avances en las pruebas piloto para el proyecto CYBELE

GMV participa en CYBELE, un proyecto financiado por la Unión Europea que tiene como objetivo innovar y crear valor en los dominios de la agroalimentación mediante la implementación de métodos de agricultura de precisión (PA) y ganadería de precisión (PLF).

Desde los inicios del proyecto, la compañía lidera uno de los nueve pilotos del proyecto para evaluar y demostrar el uso de tecnologías aplicadas a la agricultura y ganadería de precisión, enfocándose en el desarrollo de servicios climáticos para la toma de decisiones sobre la gestión de explotaciones de frutales por parte de los agricultores.

Debido a la complejidad que supone pronosticar eventos meteorológicos extremos, las pruebas, que tuvieron lugar a finales de enero, se dividieron en tres bloques: uno dedicado al pronóstico del granizo, otro al pronóstico de las heladas y el último dedicado a la fenología de cada tipo de fruta.

En el marco de estas pruebas piloto, GMV ha logrado grandes avances en la conceptualización y exploración de métodos basados en *machine learning* (ML) para el pronóstico de heladas o granizos. Estas pruebas se realizaron en dos zonas de la Comunidad Valenciana.

El trabajo desarrollado por la compañía en este piloto se apoya en datos del *Meteorological Archival and Retrieval System* del *European Centre for Medium-Range Weather Forecasts* (ECMWF) y la Agencia Española de Meteorología (AEMET).

GMV presente en la European Space Conference

GMV patrocinó la décimo tercera edición de la «European Space Conference», encuentro anual que congrega a altos representantes de entidades gubernamentales, agencias e instituciones europeas e internacionales, así como a destacados miembros de la industria.

Celebrado en formato *online* a mediados de enero, esta edición giró en torno al lema «Space Embracing a Changing World: Green, Digital, Resilience & Security» y abarcó un gran abanico de temas como fueron la situación de la industria espacial, el *New Space*, misiones de exploración espacial, aplicaciones en el ámbito de la aviación y del transporte marítimo, las telecomunicaciones y el 5G, el reto de la transición digital, los avances en la tecnología cuántica, la IA, y la estrategia económica de recuperación europea

Jesús B. Serrano, director general de GMV, participó en la presentación «The role of research in boosting European space competitiveness» junto al director general de Investigación e Innovación de la CE, Jean-Eric Paquet; el director de Tecnología, Ingeniería y calidad de la ESA y responsable de ESTEC, Franco Ongaro; el presidente de ESRE, Bruno Sainjon, y el director general de Telespazio, Luigi Pasquali. Asimismo, el director general de Espacio de GMV, Jorge Potti, formó parte de la sesión paralela «Cleaning up our orbits: accelerating the move to remove space debris», compartiendo mesa con el director de Operaciones de la ESA, Rolf Densing; la directora de Desarrollo e Innovación de la dirección general de Espacio y Defensa de la CE, Ekaterini Kavvada; el jefe de la sección del Comité, Política y Asuntos Jurídicos de la Oficina de Naciones Unidas para Asuntos del Espacio Exterior, Niklas Hedman, y el director general de la compañía D-Orbit, Luca Rossettini.

El evento además contó con la participación de diversas personalidades, así como comisarios y altos representantes de la Unión Europea y la Agencia Europea del Espacio.

GMV consolida su liderazgo en la tercera fase del mayor programa de robótica espacial de la CE

El papel desempeñado por GMV en la primera y segunda fase del clúster estratégico de investigación (Strategic Research Cluster, SRC) en tecnologías robóticas espaciales ha llevado a GMV actuar como socio estratégico en los proyectos de la tercera convocatoria

Recientemente la Comisión Europea (CE) ha hecho oficial los tres nuevos proyectos de la tercera fase del clúster estratégico de investigación (*Strategic Research Cluster*, SRC) en tecnologías robóticas espaciales, coordinado por el proyecto PERASPERA, en el marco del programa Horizonte 2020.

La primera fase de este ambicioso y pionero proyecto abordó, a través de seis proyectos distintos (tres de ellos liderados por GMV), el diseño, la fabricación y las pruebas en entornos representativos de distintos elementos robóticos comunes y de alto rendimiento, aptos para operaciones en entornos espaciales orbitales y/o planetarios.

El desafío específico de la segunda convocatoria, que está actualmente cerca de su conclusión, centra sus objetivos principales en la integración de los elementos robóticos resultantes de la primera fase y la demostración, tanto en tierra como en emplazamientos análogos a la superficie lunar, de aplicaciones de robótica espacial en distintos escenarios orbitales y planetarios.

El objetivo de esta tercera convocatoria es, por un lado, dar un paso más hacia la preparación de una demostración final en una misión orbital en lo que respecta a misiones de servicios en órbita. Por otro lado, realizar un demostrador de colaboración entre robots, en un entorno análogo a Marte, en lo referente a misiones de exploración planetaria.

El papel desempeñado por GMV en la primera y segunda fase ha llevado a la compañía a actuar como socio estratégico en estos nuevos tres proyectos resultantes de la tercera convocatoria: CoRoB-X (*Cooperative Robots for Extreme Environments*), EROSS+ (European Robotic Orbital Support Services +) y PERIOD (PERASPERA In-Orbit Demonstration). En estos proyectos, GMV mantendrá su responsabilidad sobre sistemas críticos como los sistemas de autonomía embarcados de los elementos robóticos y su capacidad de cooperación. Además, contribuye en los sistemas de guiado, navegación y control (GNC).

El proyecto CoRob-X (*Cooperative Robots for Extreme Environments*), liderado por DFKI, desarrollará y demostrará tecnologías habilitadoras para equipos robóticos multiagente, orientados a mejorar la colaboración entre diferentes robots. Mientras que los proyectos EROSS+ (*European Robotic Orbital Support Services* +) y PERIOD (PERASPERA *In-Orbit Demonstration*), liderados por Thales Alenia Space y Airbus Defence and Space GmbH respectivamente, diseñarán dos conceptos de misión de demostración de servicio y montaje en órbita con el propósito de proporcionar una solución europea que cubra tanto a los satélites encargados de proporcionar este servicio, como a los satélites que lo reciben. Todo ello basado en las tecnologías robóticas desarrolladas en la 1ª y 2ª convocatorias.

Con el relevante papel de GMV en los tres proyectos, la compañía confirma su liderazgo europeo en al área de la autonomía embarcada y GNC para aplicaciones orbitales y de superficie.

El sistema autónomo del proyecto ADE, listo para usarse en entornos nucleares

El pasado 12 de marzo tuvieron lugar con éxito las pruebas robóticas del escenario nuclear del sistema ADE.

ADE es un proyecto robótico financiado por la Comisión Europea (H2020) que se enmarca dentro del programa SRC (*Strategic Robotic Cluster*) en tecnologías robóticas espaciales. Su objetivo es desarrollar y probar un sistema robótico móvil capaz de obtener datos científicos de forma oportunista y realizar desplazamientos autónomos de larga distancia (con el objetivo de llegar a recorrer 1 km en un tiempo inferior a 6 horas). Aunque el principal caso de uso del proyecto consiste en un róver para exploración planetaria, el proyecto además incluye un caso de uso adicional orientado al mercado de robótica terrestre, que consiste en un sistema autónomo robótico que pueda ser utilizado en escenarios de desmantelamiento de centrales nucleares.

La plataforma robótica utilizada en las pruebas fue Foxizirc, robot desarrollado completamente por GMV y sobre el que se ha instalado un procesador adicional que corre la aplicación del proyecto ADE conocida como ADAM. ADAM es un módulo que provee de mayor autonomía a dicho róver, permitiendo la realización de mapas 3D de un área a explorar de forma automática (*Digital Elevation Map* o DEM), sin necesidad de ningún mapa previo. Este algoritmo de mapeo es robusto a cambios en la escena ya que el mapa se actualiza en tiempo real, otorgando al róver la capacidad de evitar nuevos obstáculos que aparezcan en escena. El sistema es capaz de detectar automáticamente «puntos calientes» de mayor radiación, analizando completamente el área bajo estudio y generando un mapa final con los niveles de radiación en cada punto. Además de la radiación, también se analizan posibles fugas en el suelo. Para ello, un agente de ciencia detecta fugas mediante el uso de redes neuronales convolucionales. Estas redes han sido entrenadas con imágenes para detectar automáticamente fugas de agua o elementos extraños en el área a explorar.

El acontecimiento fue seguido vía teleconferencia por el equipo de revisores del proyecto miembros del grupo PERASPERA(H2020), compuesto por diferentes representantes de las agencias espaciales europeas (ESA y UK Space Agency), así como por miembros de la Comisión Europea y, de manera presencial, por un representante de CDTI (Centro para el Desarrollo Tecnológico Industrial).

GMV es nuevo socio de la Asociación Española de Robótica y Automatización

GMV se une a la AER Automation (Asociación Española de Robótica y Automatización) y afianza su posición como uno de los principales actores del mercado de la automatización y la robótica industrial.

El objetivo de los asociados de la AER Automation es promover la transformación del tejido productivo nacional a través de las tecnologías de robótica industrial y automatización.

En palabras de Miguel Hormigo, director del Sector de Industria de Secure e-Solutions de GMV, «es un placer y un orgullo ser miembros de una entidad tan prestigiosa como AER Automation. Formar parte de un colectivo con grandes compañías y expertos nos ayuda a sumar esfuerzos para impulsar la transformación digital del sector industrial».

GMV participa en el arranque del proyecto GEODE

El proyecto es un paso crucial y decisivo para el desarrollo del segmento de usuarios militares del servicio público regulado (PRS) de Galileo y uno de los proyectos de cooperación en materia de defensa más ambiciosos lanzados bajo el paraguas del programa EDIDP de la Comisión Europea

Como parte del consorcio, liderado por FDC, GMV ha participado en la reunión de lanzamiento de GEODE celebrada el día 8 de febrero.

GEODE (*GalilEO for EU DEfence*) es un paso crucial y decisivo para el desarrollo del segmento de usuarios militares del servicio público regulado (PRS) de Galileo y uno de los proyectos de cooperación en materia de defensa más ambiciosos lanzados bajo el paraguas del Programa Europeo de Desarrollo Industrial de la Defensa (EDIDP) de la Comisión Europea. Cofinanciado por Bélgica, Alemania, Italia, Francia y España, GEODE cuenta con el apoyo de la UE con una subvención de unos 44 millones de euros.

El proyecto GEODE tiene como fin impulsar la competitividad de la industria de la UE en el ámbito altamente estratégico del posicionamiento, navegación, temporización y sincronización (PNT) para usos de defensa y dotar a las fuerzas armadas de la UE de capacidad para la utilización del servicio público regulado (PRS) del sistema Galileo. El proyecto será ejecutado por un consorcio formado por 30 empresas de 14 países de la UE.

El equipo industrial español, compuesto por GMV, Indra y Tecnobit, toma una responsabilidad de primer nivel en el proyecto del desarrollo completo de la solución para plataformas militares navales (receptor GNSS/PRS con módulo de seguridad y antena CRPA). GMV es la encargada de la integración del sistema receptor GNSS/PRS y, en particular, del desarrollo de todas las funciones de procesado de señal, navegación y sincronización del receptor.

GEODE proporcionará a la industria de la UE las herramientas necesarias para participar en igualdad de condiciones en el mercado PNT de defensa, en un momento en el que el carácter esencial del GPS para aplicaciones militares otorga supremacía a la industria estadounidense. Reforzará asimismo la capacidad y la autonomía militares de la UE y maximizará los beneficios del programa Galileo fomentando la adopción de su importante servicio PRS.

Este proyecto ha recibido financiación del Programa Europeo de Desarrollo Industrial de la Defensa (EDIDP) en virtud del acuerdo de subvención nº EDIDP-PNTSCC-2019-039-GEODE

Este artículo refleja únicamente la opinión del autor. La Comisión y los Estados miembros de la UE que participan en el proyecto Geode no son responsables del uso que pueda hacerse de la información que contiene

GMV incorpora nuevas funcionalidades al programa SMACS de la Armada

A finales de 2020, GMV desplegó con éxito en las instalaciones del Centro de Operaciones de Vigilancia Marítima (COVAM) en Cartagena la fase 3 del adaptador SMACS.

Esta nueva fase, adjudicada por la Jefatura de Apoyo Logístico de la Armada, demuestra su interés por seguir apoyando la red CISE de intercambio de información de vigilancia y seguridad marítima en Europa.

El proyecto, que empezó en su fase inicial como un adaptador que permitía el intercambio de información a nivel nacional entre los sistemas del Centro de Operaciones de Vigilancia Marítima (COVAM) de la Armada, del Centro de Seguimiento Pesquero (CSP) y del Centro de Coordinación Operativa (CECOP), no ha dejado de evolucionar año tras año.

El primero de los grandes hitos fue conseguir que, gracias a este proyecto, la Armada se haya convertido en el punto de conexión de la red CISE con la red de vigilancia marítima MARSUR, en la que participan entidades militares de 20 países.

El siguiente avance importante fue la conexión con los estándares MAJIIC JISR, sobre los que GMV tiene gran experiencia gracias a la familia de productos CSD (*Coalition Shared Database*) desarrollados para el Ministerio de Defensa.

En esta última fase se ha añadido un módulo de análisis del comportamiento al adaptador, lo que permitirá identificar los barcos que están realizando maniobras sospechosas. Este tipo de maniobras, como la entrada o salida de barcos en una determinada zona o la aproximación de dos barcos en mitad del mar, lanzarán una alarma en el sistema que facilitará al operador la identificación de la actividad irregular.

Ente las prioridades de la Armada está el fomento de herramientas que favorezcan la colaboración y mejoren la información disponible, por lo que GMV y Armada seguirán trabajando juntos para mejorar el sistema de manera que llegue a ser una pieza de ayuda clave para los operadores en sus tareas diarias con el objeto de garantizar la seguridad en el medio marítimo.

Un nuevo hito en el área de inteligencia, vigilancia y reconocimiento

A finales de 2020 tuvo lugar la recepción del proyecto para el desarrollo de una «Estación Embarcable Interfaz Tipo Core para ESM Cooperativa».

Equipo del proyecto tras finalizar las pruebas de integración HW

El objetivo de este proyecto es suministrar un sistema que permitirá explotar la información de trazas proporcionada por la red Link16 y por el nuevo POD de guerra electrónica de los F-18 del Ejército del Aire, denominado CORE (capacidad operacional de reconocimiento electrónico). El sistema, diseñado para operar desde tierra, incluye propiedades que permiten la experimentación embarcado en plataforma aérea como puede ser en un C-295.

Se llega a la recepción después de un complejo proceso de pruebas, tanto en ALA-35 (Base Aérea de Getafe) como en CLAEX (Centro Logístico de Armamento y Experimentación de la Base Aérea de Torrejón), donde se ha verificado la interoperabilidad del sistema en un entorno representativo del destino (componentes de comunicaciones del F-18, red JISR y protocolos de comunicaciones de la estación de tierra del POD-CORE).

El sistema desarrollado por GMV recogerá las trazas ESM (*Electronic Support Measures*) de diferentes fuentes, realizando procesos de fusión y generando mensajes para misiones cooperativas CESMO (*Cooperative ESM Operations*) según el estándar de interoperabilidad STANAG 4658.

Este sistema avanza un peldaño más en el uso de este estándar, que una vez incorporado facilitará a los sistemas del Ministerio de Defensa integrarse en misiones multinacionales con sensores y nodos de proceso de países aliados.

Puertos del Estado renueva su confianza en GMV

GMV renueva el contrato para el mantenimiento de la red de Estaciones AIS de Puertos del Estado incorporando diversas funcionalidades orientadas a mejorar la explotación portuaria, así como la gestión de las ayudas a la navegación

Un año más Puertos del Estado ha confiado el mantenimiento de la red de estaciones AIS (*Automatic Identification System*) a GMV.

La red AIS de Puertos del Estado tiene como objeto permitir conocer a los usuarios los datos de identificación de buques, su posición, rumbo, velocidad, tipo de carga, puerto de destino, hora de llegada y otros datos análogos en tiempo real, incorporando diversas funcionalidades como valor añadido, orientadas a la explotación portuaria y a la gestión de las ayudas a la navegación. Además, toda la información que llega, queda almacenada, lo que permite su utilización posterior con fines estadísticos, investigación de incidentes o realización de estudios.

Toda la información recogida diariamente por la red de Puertos del Estado sobre más de 3.000 buques en las aguas españolas, se muestra en la aplicación ***ShipLocus***®, desarrollada por GMV. Esta información, emitida por los dispositivos AIS de a bordo de los buques, es recibida mediante varias estaciones ubicadas en la costa cuyo mantenimiento también es responsabilidad de GMV.

Las funcionalidades proporcionadas por esta red van destinadas, principalmente, a los departamentos de explotación de las autoridades portuarias y a los de ayudas a la navegación, pero adicionalmente Puertos del Estado también comparte esta información con otras entidades tales como Guardia Civil, Armada y Salvamento Marítimo.

Además de las funciones de observación y monitorización del tráfico marítimo y portuario, la red permite proporcionar varios servicios a los buques, tales como la posibilidad de intercambio de mensajes con los buques para su utilización por parte de los centros de control de los puertos, la difusión de datos meteorológicos y oceanográficos procedentes de las redes de medida de Puertos del Estado, el envío de mensajes de aviso a los buques para evitar colisiones con boyas de balizamiento o medida de oleaje, el envío de mensajes a los buques informando de incidencias en las ayudas a la navegación.

Dentro del alcance del nuevo contrato, ***ShipLocus***® reportará las emisiones en tiempo real y agregadas producidas por los diferentes tipos de barco en las distintas etapas de la navegación.

GMV se consolida como empresa referente en redes y sistemas EUCI

A finales de 2019, la Agencia Europea de Defensa (EDA) adjudicó a GMV un contrato marco para durante los próximos años diseñar y desplegar sistemas de comunicación e información (CIS) que permitan el almacenamiento, procesado e intercambio de información clasificada (EUCI) hasta nivel EU SECRET.

El objetivo de la EDA es disponer de dichos sistemas EUCI-CIS para manejar la información clasificada tanto a nivel interno dentro de la Agencia como compartirla con instituciones y organismos gubernamentales de los Estados miembros de UE y con otras entidades implicadas en proyectos que requieran del acceso a dicha información.

Bajo dicho contrato, como integrador de los sistemas, GMV es punto de contacto único y la empresa responsable de realizar y analizar los requisitos de usuario y de sistema. Además, evaluará amenazas, vulnerabilidades y riesgos identificando las correspondientes medidas de mitigación. También generará la documentación necesaria para el proceso de acreditación, así como dará soporte durante el mismo y se ocupará del diseño, implementación y despliegue de dichos sistemas.

Durante 2020, GMV ha trabajado en el diseño y en la fase preparatoria para la acreditación del primero de los sistemas, que permitirá a la agencia el manejo de información clasificada hasta el nivel EU SECRET y que será desplegado y acreditado pasando a operación durante el año 2021.

En paralelo, a principios de 2021 un segundo sistema para el manejo de información hasta nivel EU RESTRICTED ha entrado en fase de preparación y diseño con el objetivo de estar operacional a principios de 2022.

El diseño y despliegue de estos sistemas se desarrolla de acuerdo al marco legal de la UE para el manejo e intercambio de EUCI con la acreditación final por parte de la Security Accreditation Authority (SAA) del General Secretariat of the Council (GSC).

GMV será también responsable de proporcionar servicios de soporte técnico, mantenimiento, capacitación y formación continua del personal de la EDA.

GMV participa en el taller de la EDA sobre capacidades de inteligencia, vigilancia y reconocimiento

En junio de 2019, la Agencia Europea de Defensa (EDA) publicó once casos de contexto estratégico (*Strategic Context Cases-SCC*) como una guía para implementar las prioridades de desarrollo de capacidades acordadas por los Estados miembro en 2018.

Estos SCCs están siendo usados para definir las prioridades de inversión en las futuras iniciativas de defensa europea (como la cooperación permanente estructurada PESCO y los fondos de defensa europeos o EDF).

En este contexto, la EDA está organizando una serie de talleres para cada uno de estos casos de contexto estratégico con el objetivo de proporcionar información a la Industria sobre el SCC correspondiente y recopilar sus contribuciones para la definición adicional de las líneas de trabajo en el área.

El día 21 de enero tuvo lugar, de manera telemática, el taller dedicado a la superioridad de la información y más concretamente a las capacidades de inteligencia, vigilancia y reconocimiento. El artículo técnico «Intelligence, Surveillance and Reconnaissance Networked Capabilites», preparado por GMV, fue uno de los seis seleccionados para ser compartido durante el taller y su presentación ante representantes de organismos gubernamentales, de la industria y de la academia fue acogida con mucho interés.

Esta actividad permite seguir consolidando y potenciando la presencia de GMV en las áreas de la industria de defensa donde la compañía es referente e influir en la definición de las líneas de inversión prioritarias en los nuevos programas de defensa europeos.

Opinión

Aprobado en España el Reglamento NIS

El día 28 de enero se aprobó el Reglamento NIS en España. Este reglamento establece requisitos mínimos de ciberseguridad para las organizaciones que prestan servicios críticos a la sociedad. Este esperado reglamento profundiza en la trasposición de la Directiva NIS de la UE y su integración en el marco legal. Si bien este reglamento se refiere solo a organizaciones que prestan sectores críticos, probablemente sea adoptada como referencia en el mercado.

El Reglamento NIS establece una línea de base de medidas mínimas de ciberseguridad que deben ser cubiertas por las organizaciones, que combinan medidas ya comunes junto con otras medidas que solo habían adoptado las organizaciones con más madurez.

La primera novedad es la obligación de las organizaciones de notificar sus ciberincidentes a la Administración. Obligación ya establecida por la GDPR para incidentes de privacidad que ahora se amplía a incidentes de ciberseguridad. Se establece también la necesidad de colaboración entre organización y administración para la resolución del incidente, combinando las propias capacidades de la organización con la coordinación de la administración en la resolución del incidente y en la alerta temprana a otras organizaciones que pudieran también tener un incidente similar.

La segunda novedad dota a la administración de capacidad de supervisión del cumplimiento de este reglamento, mediante puntos de comunicación entre la administración y la organización. Además, le otorga capacidad auditora y la necesidad de reporte por la organización a la administración de su estado de ciberseguridad.

La tercera novedad determina que la organización cuente con un responsable de seguridad de la información como punto de contacto con la Administración y como responsable de que la organización cumpla con esta regulación. El reglamento establece los requisitos de formación y experiencia exigibles a esta figura, así como la obligación para la organización de aportar recursos, autoridad e independencia suficientes para poder desarrollar las responsabilidades del reglamento.

Mariano J. Benito,
CISO de Secure e-Solutions de GMV

> El Reglamento NIS establece una línea de base de medidas mínimas de ciberseguridad que deben ser cubiertas por las organizaciones

Respecto de las medidas mínimas, se trata de materias comunes y conocidas en ciberseguridad: tener una política de seguridad, aplicar medidas de seguridad de seguridad física, técnicas y organizativas, disponer de planes de continuidad de negocio, la gestión de riesgos, la mejora continua o detectar y gestionar sus ciberincidentes.

La publicación de este reglamento pone de actualidad el valor de los más de 25 años de experiencia en seguridad de GMV y su capacidad de entrega a sus clientes de servicios del máximo valor añadido.

Grupo Carreras, ciberseguridad en sectores esenciales durante la pandemia

La protección de las infraestructuras críticas y la prestación de los servicios esenciales se han convertido en una prioridad para los estados. Para abordar este tema, la Fundación Borredá organizó el Congreso de Protección Integral de Servicios Esenciales e Infraestructuras Críticas (PISE) durante el pasado mes de noviembre.

La Fundación Borredá contó con el apoyo tanto de representantes de la administración española como del sector privado, a través de sus socios protectores, del que GMV forma parte. Más de 1.000 profesionales se registraron al congreso, que pudieron asistir de forma virtual a un programa compuesto por interesantes ponencias que abordaron la gobernanza de la seguridad, la ciberseguridad y el modelo de protección de los servicios esenciales.

Dentro del panel «Experiencias y Soluciones aplicadas», GMV compartió junto a Grupo Carreras su experiencia sobre el papel de la ciberseguridad en sectores esenciales durante la pandemia, enfocado en el sector logístico.

Javier Ibáñez, CIO y líder de Transformación Digital del Grupo Carreras, y Javier Hidalgo, arquitecto de soluciones del sector Industria de GMV, presentaron el proyecto conjunto de ambas compañías en materia de ciberseguridad. Ibáñez explicó el papel de la seguridad como elemento principal en el plan de transformación digital de la compañía, debido a la gran cantidad de información que manejan y cómo desde el principio apostaron por los servicios de GMV.

En concreto, GMV apoya al Grupo Carreras en la evaluación del estado de la ciberseguridad en el proyecto de gestión del CERT (*Computer Emergency Response Team*) de seguridad y en la formación y evangelización en ciberseguridad.

GMV adapta los cajeros automáticos al futuro con un máximo nivel de seguridad

GMV estuvo presente en BankSec, el encuentro virtual organizado por Retail Banking Research (RBR) en diciembre de 2020 para analizar las características de los ciberataques encontrados en las redes de cajeros automáticos y recomendar las medidas de protección más adecuadas ante esas amenazas.

Después de examinar los ataques más recientes, es de destacar que la mayor parte de las vulnerabilidades explotadas tienen su origen en la utilización de puertas traseras que las propias entidades se ven forzadas a crear para facilitar la operación de sus cajeros. Por ejemplo, la posibilidad de conectar los USB a los cajeros es un punto débil que muchas entidades se ven obligadas a permitir para que los técnicos puedan realizar labores de mantenimiento *on site*.

Si analizamos las características de las redes de cajeros, quizás el elemento que mejor los defina es la estabilidad: estabilidad del software, de los datos, de las transacciones, de la ejecución en general. Y a la vez sabemos que los ataques suponen en líneas generales un terremoto a esa estabilidad: transacciones incompletas, secuencias de ejecución modificadas, importes anormalmente elevados o reducidos, etc.

Estas características tan particulares del entorno hacen que la utilización de tecnologías de análisis del comportamiento y detección de anomalías sean especialmente indicadas para estos casos. Para ello, es necesario que se basen en un comportamiento estable y bien conocido de los sistemas, sin sufrir alteraciones provocadas por la heterogeneidad de las redes de cajeros en cuanto a fabricantes y modelos. En este contexto, la capa XFS aporta esa estabilidad y uniformidad.

Pero en muchos casos la detección de anomalías no es suficiente para detener un ataque. De nuevo la capa XFS constituye el punto de entrada perfecto para, además de analizar el comportamiento y detectar anomalías, tomar las medidas necesarias para bloquear ese comportamiento sospechoso.

GMV ha desarrollado un nuevo producto de seguridad para cajeros, ***Checker XFS Filtering***, que, al nivel de la capa XFS del cajero, implementa una solución completa que integra análisis del comportamiento del cajero, detección de anomalías y filtrado de acciones sospechosas. Esta nueva solución de GMV viene a completar su producto de seguridad para cajeros automáticos, ***Checker ATM Security***, con el que se integra de forma natural dotando a los cajeros del máximo nivel de seguridad.

Opinión

Ciberataques *Man-In-The-Middle* en el entorno industrial

La adopción de tecnologías de la información en el ámbito industrial lleva siendo una constante durante las últimas décadas. Cada vez más empresas apuestan por la introducción de nuevos sistemas de información en sus sistemas productivos con el objetivo claro de aprovechar las ventajas competitivas que ello conlleva, siendo las más destacadas el asegurar la producción, reducir costes y ganar en eficiencia. Sin embargo, este proceso, tan necesario como inevitable, comporta la introducción de nuevos riesgos en los sistemas de producción.

Por su propia dinámica histórica, la seguridad en los entornos industriales ha estado más orientada a la seguridad por oscuridad que a la adopción de sistemas de gestión de la seguridad como se entiende en el sector de las tecnologías de la información. Si bien esta estrategia podía ser justificable en un inicio, la irrupción de las TI y su convergencia con los sistemas de producción —lo que provoca un inevitable crecimiento de la superficie de ataque a dichos sistemas— ha generado un escenario donde el riesgo de sufrir ciberataques ha crecido de manera dramática.

Por suerte, dichas amenazas son bien conocidas en el ámbito de la TI convencional y difieren en poco en el ámbito específico de la IoT en entornos industriales en su tipología, si bien su desarrollo en dicho ámbito y cómo dichas amenazas han de afrontarse sí requieren de un tratamiento más adaptado al entorno.

Entre estas amenazas destacaremos las de tipología *Man-in-the-Middle* (MITM), donde su estrategia de ataque se basa en la interceptación de comunicaciones entre múltiples dispositivos IoT, falseando o alterando las comunicaciones y provocando tanto mal funcionamiento de los sistemas de producción como la toma de decisiones erróneas por los operadores basadas en dicha información alterada.

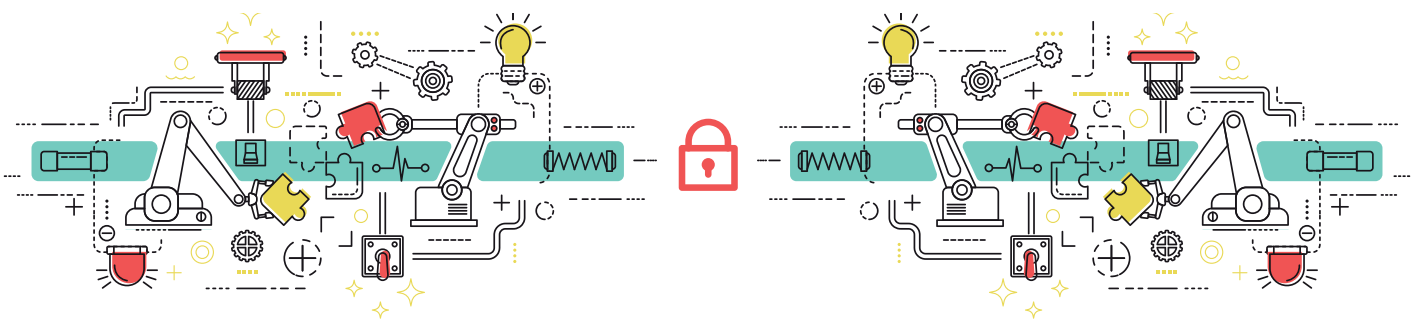
¿Cómo es posible protegerse de estos ciberataques de tipo MITM?
Para ello destacamos aquellos aspectos que son clave en un escenario de producción industrial.

- Estableciendo un diseño de seguridad desde el inicio del despliegue de los sistemas IoT y no como un añadido posterior.
- Cifrado de comunicaciones de extremo a extremo entre dispositivos IoT y plataforma de gestión con una adecuada validación de credenciales, preferentemente basada en certificados de dispositivo.
- Estableciendo conexiones seguras mediante VPN, en caso de necesitar comunicaciones con plataformas externas al entorno industrial.

Javier Hidalgo Sáez.
Arquitecto de soluciones sector Industria de Secure e-Solutions de GMV

Cada vez más empresas apuestan por la introducción de nuevos sistemas de información en sus sistemas productivos, lo que comporta la introducción de nuevos riesgos en los sistemas de producción

- Desterrar el uso de confianza automática en nuevos dispositivos añadidos a la plataforma, realizando una integración controlada y programada de nuevos dispositivos.
- Instruyendo a los empleados en la importancia de la seguridad en los entornos IoT, al igual que en el resto de entornos TI de la empresa.



Cómo hacer frente a los riesgos y amenazas en la era digital

A finales de enero, AENOR y GMV participaron en una jornada para debatir sobre los nuevos retos ante las nuevas amenazas y riesgos TIC a los que se están enfrentando las organizaciones en la era digital y en especial durante la época de pandemia que estamos viviendo. Se hizo especial énfasis en la implantación y certificación de estándares internacionales ISO como palanca para que las organizaciones obtengan altos niveles de seguridad, confianza y resiliencia, que les permitan afrontar los desafíos de la crisis actual o de futuras y que aseguren una sólida transformación digital orientada a objetivos de negocio.

Boris Delgado, gerente de certificación TIC en AENOR, presentó la Plataforma de Confianza TIC como una solución a los riesgos TIC actuales y futuros y como parte del ecosistema digital de AENOR. Su objetivo es proporcionar seguridad y confianza ante la actual crisis o futuras, así como la vuelta a la «nueva normalidad» con las garantías de resiliencia, continuidad y ciberseguridad en los sistemas y servicios de TIC. Para Delgado, los estándares internacionales están ayudando a que, en la situación de pandemia actual, las organizaciones cumplan sus objetivos de negocio, sepan enfrentarse a los nuevos riesgos y amenazas y estén preparados no solo para ahora, sino de cara al futuro.

GMV, como empresa pionera en la implantación y certificación de estándares ISO, como la 27001 de seguridad o la nueva 27701 de privacidad, aportó su experiencia a través de Mariano J. Benito, como CISO de Secure e-Solutions de GMV. Benito explicó cómo fue la reacción de la compañía ante la pandemia de coronavirus y destacó que «GMV ya había valorado escenarios de crisis y teletrabajo similares al ocurrido, solo tuvimos que activar determinadas tareas que ya teníamos planificadas y entrenadas. Habíamos previsto lo que podíamos necesitar y habíamos identificado y resuelto aquellos problemas de seguridad que podíamos encontrarnos». La aplicación preventiva, sostenida y rigurosa de sistemas de gestión basados en estándares internacionales proporciona seguridad para estar preparados ante estas situaciones.

Una de las últimas normas que se han publicado en ISO en este ámbito es la ISO27701 sobre privacidad de datos. GMV ha sido la primera en obtener e implantar esta certificación por parte de AENOR. Para GMV, la ISO27701 ha supuesto una herramienta para conseguir que la orientación a la privacidad que exige la ley permease dentro de la organización a través de los sistemas de gestión que ya teníamos implantados. Benito destacó el papel de AENOR como auditor «ha sido fundamental para aportarnos un criterio independiente, sólido y profesional, respecto de cómo esa necesidad que teníamos de privacidad aplicada a través de nuestros sistemas de gestión estaba cumpliendo con los requisitos del estándar».

GMV, identificado como «Key Innovator» por el innoradar de la UE

El Radar de la Innovación de la Comisión Europea reconoce a GMV por sus desarrollos e investigaciones en la deformación natural y la manipulación de imágenes médicas en tres dimensiones

El Radar de la Innovación de la Comisión Europea (*https://www.innoradar.eu*) ha reconocido a GMV como «Key Innovator» por sus desarrollos e investigaciones en la deformación natural y la manipulación de imágenes médicas en tres dimensiones, que resultarán de gran ayuda a los cirujanos en su entrenamiento con cirugías, así como en su preparación y planificación.

La relevancia de las investigaciones realizadas por GMV estriba en haber sido capaz de modelar complejas relaciones entre estructuras anatómicas y su comportamiento elástico, desarrollando algoritmos para capturar estas complejidades y tratar imágenes médicas, ello con una gran aproximación al tiempo real.

Para Carlos Illana, responsable de producto en Secure e-Solutions de GMV, «entre los desarrollos de GMV que han sido valorados por la Comisión, cabe destacar los algoritmos de simulación de deformación y corte sobre imagen médica volumétrica, todo un reto que supondrá un gran avance para la planificación quirúrgica, que en estos momentos sólo contempla estructuras óseas». Esta innovación, única en el mundo, «no sería posible sin el trabajo conjunto de ingenieros altamente especializados y con conocimientos pioneros en el ámbito empresarial y de organismos públicos de investigación a nivel mundial».

El Innoradar de la Comisión Europea se ha creado para identificar innovaciones digitales y entidades innovadoras de alto potencial que participan en proyectos de investigación financiados con fondos comunitarios. Esta herramienta persigue, por un lado, dar visibilidad de los proyectos a potenciales inversores que hagan posible la puesta en el mercado de estos desarrollos para su comercialización y fomenten la creación de un ecosistema innovador. Por otro, responde a un ejercicio de transparencia que permite a la sociedad conocer donde se destina la financiación de la UE.

Las investigaciones por las que ha sido reconocida GMV se están desarrollando en el marco del proyecto RAINBOW, cuyo objetivo es la investigación para el desarrollo de una nueva generación de simuladores clínicos, prácticos y fáciles de usar por los especialistas, que contribuyan al diseño y la aplicación de una medicina personalizada.

En el marco del proyecto, GMV ha contribuido al desarrollo de estas herramientas que pueden ser aplicadas en el diagnóstico, pronóstico, seguimiento, entrenamiento quirúrgico, planificación, orientación, diseño de prótesis, operaciones de implantes y dispositivos médicos. Esta nueva generación de herramientas de simulación biomecánica podrá ser manejada por los médicos sin necesidad de la intervención de los técnicos. RAINBOW es un proyecto incluido en la Innovative Training Networks (ITN) del programa Horizonte 2020.

RAINBOW
Rapid Biomechanics Simulation for Personalized Clinical Design
A Marie Skłodowska-Curie European Training Network

Navegación y algoritmos: revolución en los quirófanos

Las nuevas tecnologías de navegación, los algoritmos de simulación quirúrgica y la imagen intraoperatoria han contribuido notablemente a que las cirugías puedan realizarse con mayor precisión y garantía de resultados en términos de salud. De este modo, proporcionan mayor seguridad durante la intervención, una más pronta recuperación y, por lo tanto, una mejora en la experiencia vivida por el paciente.

En palabras de la doctora Marisa Gandía, neurocirujana del Hospital Universitario La Paz de Madrid, «la cirugía guiada por imagen ha supuesto una revolución». En concreto, la navegación en el ámbito de la cirugía es comparable a lo que «el GPS ha significado para el mundo en general», señala Carlos Illana, responsable de producto en Secure e-Solutions de GMV.

En el caso concreto de la cirugía mínimamente, donde el cirujano trabaja apoyándose en la imagen médica en vivo, la tecnología le permite la planeación, simulación y seguimiento intraoperatorio a través de la visualización en tiempo real de imágenes tridimensionales. Con los sistemas de navegación, este especialista puede conocer con exactitud la posición del instrumental o revisar el campo quirúrgico en una imagen tridimensional del paciente. Las técnicas computacionales son un avance indispensable que permite optimizar la planificación en el preoperatorio, así como mejorar la precisión y calidad de la técnica quirúrgica. En el marco del proyecto Naviphy, GMV está investigando para ofrecer imágenes y parámetros en tiempo real de las acciones que está llevando a cabo el cirujano en la intervención, así como de los posibles cambios que sufrirá la anatomía del paciente durante la operación.

Como incide Carlos Illana, «los sistemas de navegación quirúrgica y simulación aplicados a la cirugía mínimamente invasiva están siendo utilizados cada vez más en las operaciones porque aportan más seguridad y precisión». Aun así, «queremos llevar esta tecnología al siguiente escalón y mejorar los sistemas de posicionamiento actuales, así como incorporar técnicas de simulación que permitan reducir la necesidad de imagen sin penar la precisión y la seguridad». Para ello se está trabajando en el marco del proyecto Naviphy.

Como explica la dra. Gandía, en la cirugía mínimamente invasiva mediante neuronavegación se posiciona un sistema tubular y se fija la localización para operar. En estas cirugías «los tejidos se van separando mediante dilatación y no a través de la desinserción amplia de la musculatura, el acceso al lecho quirúrgico es mucho menos agresivo». Esto, unido a que la incisión que se practica al paciente es más pequeña, «el riesgo de infección y el dolor se reducen drásticamente, lo cual incide en una más rápida recuperación. La mayor parte de los pacientes en las primeras 24 horas empiezan a caminar y se reincorporan a su actividad habitual, mucho antes que con la cirugía convencional. En definitiva, menor daño, dolor, sangrado e infección».

GMV participa en el proyecto Naviphy, enmarcado en la convocatoria I+D+I Retos Investigación del Ministerio de Ciencia, Investigación y Universidades, y subvencionado por UE a través de los fondos FEDER. El objetivo es lograr mayor precisión en cirugías de mama, cerebro y maxilofacial, así como en radioterapia intraoperatoria y braquiterapia. Además busca explorar nuevas tecnologías de navegación, desarrollar algoritmos de simulación quirúrgica y evaluar el uso de las diferentes tecnologías de imagen intraoperatoria.

GMV participa en la publicación «Asistencia sanitaria no presencial» editado por ProPatiens

El 29,5 % de los pacientes crónicos utilizaron la telemedicina durante el confinamiento domiciliario por la pandemia de la COVID-19. Las mujeres aprovecharon las posibilidades de la medicina *online* más que los hombres, en un 32,7 % de los casos frente al 25,3 en los varones. Son datos que recoge el estudio «Uso de internet durante el confinamiento para consultas no presenciales con su médico o profesional sanitario que le atiende», elaborado por el Instituto ProPatiens y recogido en el e-book gratuito «Asistencia sanitaria no presencial», que cuenta con la colaboración de GMV, cuya apuesta firme por ella se concreta en su plataforma de asistencia sanitaria no presencial ***Antari***.

La publicación incluye una entrevista a Carlos Royo, director de Estrategia de Salud de GMV y presidente de la Comisión de Salud Digital de AMETIC, en la que pone el acento en «la urgencia de impulsar la trasformación digital del sistema nacional de salud, tanto para conseguir que sea sostenible como para poder colocar al ciudadano en el centro con el empoderamiento suficiente que le permita gestionar y decidir sobre qué es lo que cree más conveniente para su salud, obviamente acompañado en este viaje por sus profesionales».

GMV en el pódium de los TOP 10 de la RIO

La consultora Apex Market Research, en su último estudio de mercado realizado a nivel mundial sobre radioterapia intraoperatoria (RIO), sitúa a GMV entre los Top 10 en la categoría de empresa innovadora. En la matriz empleada para la investigación, las compañías con esta clasificación se corresponden con aquellos proveedores que han demostrado innovaciones sustanciales en sus productos en comparación con sus competidores.

La radioterapia intraoperatoria es una técnica de alta precisión en la cual se administra una fracción única y elevada de radioterapia durante un acto quirúrgico, sobre el lecho tumoral/residuo microscópico o sobre el tumor macroscópico en caso de tumores irresecables. Con ella se visualiza de forma directa el lecho a irradiar y deja fuera del campo de irradiación los tejidos sanos circundantes.

La creciente incidencia del cáncer, los avances tecnológicos y las ventajas que ofrecen las aplicaciones de la radioterapia intraoperatoria son los principales factores que están impulsando el crecimiento del mercado global. La consultora prevé en su estudio que la radioterapia intraoperatoria alcanzará los 67,8 millones de dólares en 2024, creciendo a una tasa anual del 7 % de 2019 a 2024.

GMV cuenta con el único planificador radioquirúrgico del mercado, ***Radiance™***, una herramienta que mejora la seguridad del tratamiento radioterápico intraoperatorio (RIO), ya que facilita al especialista el análisis completo del paciente y la toma de decisiones previa a la intervención quirúrgica. Además, identifica el tratamiento óptimo para cada uno de ellos (medicina personalizada y traslacional).

GMV se encuentra entre los líderes mundiales gracias a ***Radiance™*** y a sus alianzas comerciales con otros líderes del mercado como son Carl Zeiss, Meditec AG (Alemania) e IntraOp Medical Corporation (USA). Este innovador software ofrece todos los datos necesarios para documentar la intervención, ya que calcula los parámetros exactos necesarios para aplicar la radioterapia en el propio quirófano antes de una operación. Proporciona imágenes de alta calidad multiplanar (MPR) y visión tridimensional (3D) del paciente y permitela visualización simulada del resultado del tratamiento.

Tecnología para compartir conocimiento en la gestión e investigación sanitaria

La herramienta desarrollada por GMV, ***uTile PET*** (*Privacy-Enhancing Technologies*), permite a hospitales, centros de investigación e industria farmacéutica compartir conocimiento sin necesidad de exponer los datos ni moverlos de las entidades donde se generan. Al aplicar métodos criptográficos avanzados que mantienen los datos cifrados mientras se realizan todos los cómputos necesarios mejora la precisión de las técnicas de inteligencia artificial y garantiza al cien por ciento la anonimización de los datos. Esto supone un avance de gran impacto para aplicar en la gestión sanitaria.

Asimismo, en la gestión sanitaria e investigaciones clínicas y farmacológicas permite salvar los obstáculos que suponen los «silos de datos», donde se almacena la información de salud de los pacientes y las distintas normativas nacionales y trasnacionales que prohíben compartir datos o trasladarlos fuera de los países impidiendo su agregación. Con ***uTile PET*** es posible obtener información tan crucial como el valor de los biomarcadores, pronósticos, edad media de los pacientes, de los tratamientos clínicos,etc. todo ello sin comprometer la privacidad de los datos de los pacientes.

Con ***uTile*** no hay que elegir entre privacidad de los datos y la posibilidad de utilizarlos, ya que mantiene los datos cifrados mientras se realizan todos los cómputos necesarios, permaneciendo protegidos por las organizaciones, ya sea *on premise* o *cloud*.

GMV suministra los sistemas AVLS y DMS para el tren ligero de Jerusalén

La solución que la compañía implantará para el tren ligero de Jerusalén, se basará en el producto ***SAE-R®***, la plataforma de ayuda a la explotación desarrollada por GMV para los entornos ferroviario y tranviario

GMV ha sido recientemente seleccionada por el grupo CAF para el suministro de los sistemas AVLS (*Automatic Vehicle Location System*) y DMS (*Depot Management System*) para su proyecto de tren ligero en la ciudad israelí de Jerusalén. Este proyecto comprende la extensión de la línea roja, actualmente en operación, la cual pasará a estar gestionada por CAF en su totalidad, así como la nueva construcción de una línea adicional, la línea verde.

El proyecto global, que desarrollará el consorcio CAF – Saphir, cuenta con un alcance de 160 trenes (46 procedentes de la línea roja actual que se reformarán, más 114 de nuevo suministro), 76 estaciones y 3 depósitos. Este proyecto se completará en un plazo de 4 años y medios.

La solución que GMV implantará para el Tren Ligero de Jerusalén se basará en el producto ***SAE-R®***, la plataforma de ayuda a la explotación desarrollada por GMV para los entornos ferroviario y tranviario y ya aplicado en proyectos como la plataforma de comunicaciones para los operadores ferroviarios RENFE (España) y ONCF (Marruecos) o los sistemas tranviarios de Sydney (Australia), Varsovia (Polonia), Kaohsiung (Taiwán) y Zaragoza (España).

El sistema ***SAE-R*** a implantar contará con las funciones tradicionalmente asignadas a este tipo de sistemas como la localización precisa de la flota de trenes (tanto sobre mapa geográfico como sobre mapas sinópticos detallados de líneas y depósitos), la gestión de mensajería/comunicaciones radio (tanto con conductores como con usuarios radio portátiles y fijos), la información al viajero a bordo y en estaciones (incluyendo la definición de contenidos y escaletas de reproducción), la gestión

de conductores (control de *duties* y relevos), las operaciones de regulación del servicio más avanzadas para hacer frente a cualquier imprevisto sobre la operación y la monitorización en tiempo real de alarmas y estados tanto propios como de sistemas externos.

Todas estas funciones se combinarán con otras avanzadas y de novedosa implantación como las relativas a la operación automática de los trenes en aspectos como el establecimiento dinámico de rutas, la solicitud de prioridad en cruces, el engrase de pestaña, la apertura de puertas, la iluminación en túneles, el control de espacio disponible para bicicletas o el control/telecomando desde el centro de control de ciertos «parámetros de confort» en los vehículos (aire acondicionado, control de volumen en equipamiento de información al viajero, nivel de luminosidad a bordo, etc.).

Como módulo integrado en el sistema ***SAE-R*** se encuentra el *Depot Management System* (DMS), que se gestiona desde las mismas aplicaciones de usuario que el módulo AVLS con el objetivo de una mayor eficiencia operativa. La función principal del módulo DMS será la gestión eficiente de movimientos de trenes (entradas/salidas a/de línea) y ocupación de vías en los distintos depósitos. Todo esto en base a un conjunto de políticas de ocupación de vías a definir por la empresa operadora y a la monitorización en tiempo real del estado de elementos del sistema de señalización instalado en depósitos (señales, agujas, contadores de ejes, circuitos de vía...).

El sistema ***SAE-R*** de GMV se instalará en un entorno multisistema en el que se integrará funcionalmente con multitud de sistemas externos tanto en el centro de control (SCADA, CTC, RADIO LTE, CMMS, Scheduling Tool, MOT – Ministry of Transport...) como a nivel embarcado (TCMS, Radio LTE, RRS- Route Request System, TPS – Traffic Priority System, ATP, PCS – Passenger Counting System, CCTV, Ticketing,etc.). La implementación de estas interfaces, salvo en casos especiales, se encontrará basada en el uso de estándares de comunicación como BUS NAOS, TRDP o SIRI.

Todos los trenes serán dotados de unidades embarcadas, diseño y fabricación de GMV, así como de terminales táctiles en ambas cabinas como HMI para conductor.

Esta tecnología embarcada en los trenes se completa con la instalación en las dependencias centrales de un centro de control basado en un conjunto de servidores en entorno virtualizado y *workstations* para el seguimiento y análisis de la operación por la empresa operadora de la red de transporte. Además, funcionará tanto en tiempo real como de forma diferida, siendo esta última puesta a disposición de sistemas externos para el cálculo de valores KPI relativos a la operación del sistema.

Tanto a nivel de centro de control como a nivel embarcado, el sistema ***SAE-R*** se encontrará redundado (filosofía *failover*) y asegurando la alta disponibilidad del sistema ante la aparición de errores puntuales en alguno de sus componentes.

Además, tanto a nivel de centro de control como a nivel embarcado, el producto ***SAE-R®*** contará con las más avanzadas técnicas de ciberseguridad. En concreto, con el sometimiento del sistema al análisis de vulnerabilidades de ciberseguridad por una empresa externa especializada en dicho campo.

GMV, responsable del sistema de transporte a la demanda en Castilla y León

El pasado mes de enero GMV resultó de nuevo adjudicataria del contrato de la operación y mantenimiento del sistema de transporte a la demanda en Castilla y León. Se trata de un contrato de una duración de dos años con una posible prórroga de 23 meses.

El sistema de transporte a la demanda está basado en ofrecer un servicio de transporte de forma eficiente en zonas geográficas con gran dispersión poblacional y baja densidad en cuanto a número de habitantes, como es el caso de Castilla y León.

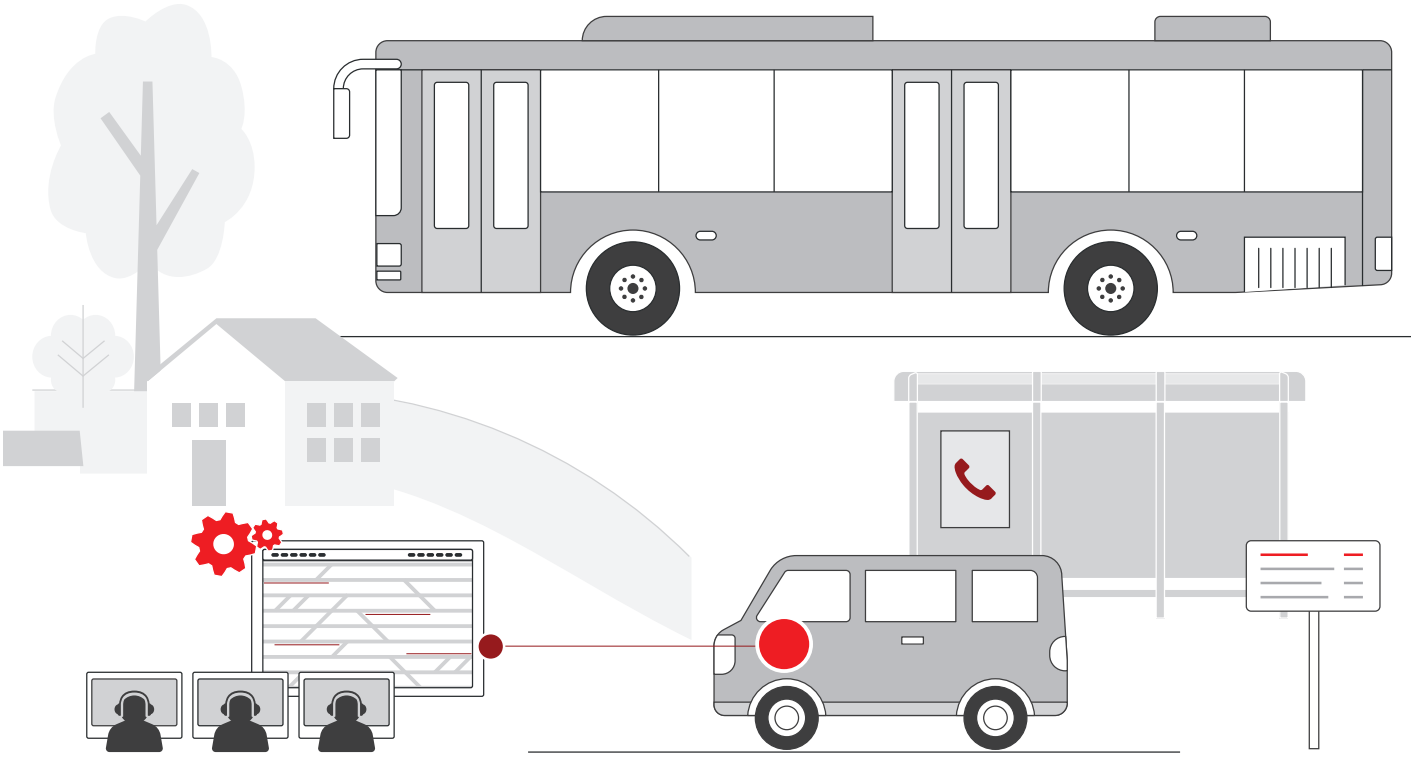
Esta modalidad de transporte supone un importante ahorro energético, debido a los kilómetros que se han dejado de realizar, puesto que los vehículos sólo circulan por aquellas localidades donde se ha concertado la reserva. De esta forma, se logra una mayor eficiencia no solo económica sino también medioambiental.

La central de reservas de transporte a la demanda de la Junta de Castilla y León, que está situada en GMV en el Parque Tecnológico de Boecillo (Valladolid), contará con una ampliación en el número de operadores y refuerzo durante los meses de verano cuando la tendencia de uso de transporte en las zonas rurales es notablemente creciente. Además, un nuevo sistema de calidad en la grabación de las llamadas aportará más visibilidad en la identificación y medición de la calidad de servicio ofrecida a los usuarios.

La plataforma de la central de reservas gestiona una flota de 327 autobuses y da cobertura a más de un millón de habitantes, 5.015 emplazamientos, 123 zonas operativas, 1.944 rutas en servicio. Asimismo o gestiona 250.000 desplazamientos de media anuales aproximadamente.

Hasta el momento, las reservas para solicitar el uso del servicio se realizaban únicamente de forma telefónica llamando a un número de teléfono gratuito. Sin embargo, en la renovación del proyecto se contempla la puesta en marcha de una web *responsive* de usuario donde cualquier ciudadano a través del móvil podrá realizar la solicitud. Además, podrá consultar información como itinerario de rutas o mensajes informativos, entre otras funciones.

Esta renovación consolida a GMV como la empresa española de sistemas inteligentes de transporte con mayor experiencia en este servicio. Así lo demuestran los 17 años de trabajos realizados en el mundo del transporte a la demanda, lo que pone de manifiesto un gran conocimiento en el diseño, la puesta en marcha y el mantenimiento de este tipo de sistemas en el mundo rural.



GMV suministrará el SAE y billetaje para Vectalia en Galicia

Vectalia confía en GMV para el suministro de su sistema de ayuda a la explotación (SAE) y de billetaje también en las concesiones que le han sido adjudicadas dentro del segundo bloque concesional, licitado por la Xunta de Galicia.

Este nuevo proyecto con Vectalia permite a GMV consolidarse con uno de los clientes estratégicos de la renovación concesional en Galicia y le sitúa, a su vez, como proveedor tecnológico de referencia de esta y otras empresas concesionarias que operan en la región.

La Xunta de Galicia se encuentra inmersa en un proceso de renovación concesional en toda la comunidad a través de dos concursos públicos en los que las empresas operadoras en el ámbito de Galicia renovarán o conseguirán nuevas concesiones que deberán explotar durante 10 años.

En este contexto, Vectalia ha contratado a GMV el suministro del sistema de ayuda a la explotación (SAE) y del sistema de billetaje no sólo para los 16 autobuses pertenecientes a la concesión adjudicada dentro del primer bloque concesional licitado por la Xunta de Galicia, sino también para los 51 autobuses adjudicados dentro del segundo bloque, que están dando servicio desde finales de 2020.

Técnicamente, GMV equipará los autobuses de Vectalia con una expendedora de billetes que permitirá la utilización de las tarjetas de transporte sin contacto de la Xunta de Galicia. Además, incorporará también tecnología de pago EMV y lector de códigos QR, que posibilitará su utilización como equipo embarcado SAE.

A nivel de centro de control, GMV suministrará sus sistemas de *backoffice* de billetaje y de SAE que, a su vez, reportarán la información de explotación a los sistemas centrales de la Xunta de Galicia.

ALSA renueva con GMV el sistema de pago en el transporte de Almería

Tras haber sido seleccionados por ALSA en noviembre de 2018 para modernizar el sistema de billetaje de los autobuses de transporte urbano en la ciudad de Almería, GMV renueva la confianza de ALSA y del Consorcio de Transportes del Área de Almería (CTAL) y firma un contrato para la actualización del sistema de venta y validación (SVV). La compañía instaló este sistema en 2001.

La nueva contratación incluye el suministro de expendedoras embarcadas ***ETC606i-8*** para una flota de 60 vehículos. Estas permitirán la venta de billetes sencillos y la validación de la actual tarjeta de transportes de la filial de ALSA, SURBUS, así como las tarjetas *Mifare Classic* y la nueva *Desfire* de la Red de Consorcios de Transporte Andaluces (RCTA).

La expendedora dispondrá de receptor GPS y *modem* 3G integrado. Sin embargo, se utilizará un *router* ya instalado por ALSA para que todas las comunicaciones se gestionen a través de una única SIM. El receptor GPS permitirá asociar datos de posicionamiento a las validaciones, que serán remitidas en tiempo real al CTAL y almacenadas en el sistema central de ALSA. También permitirá que los equipos avancen automáticamente de parada para el registro inequívoco de la parada de embarque de los pasajeros.

La gestión de recarga de las tarjetas propias de SURBUS se efectuará a bordo de los vehículos a través de 3 equipos ***ETC606i-8*** instalados en las oficinas de atención al cliente de SURBUS.

El suministro incluye también 6 terminales de inspección en formato *smartphone* rugerizado (resistente a golpes) para la gestión de inspecciones sobre las tarjetas SURBUS y tarjetas de la RCTA. Además, inspeccionará la emisión de sanciones a los usuarios en situación de fraude a través de una impresora portátil.

El sistema central incluye aplicaciones para la configuración del sistema, procesado de datos, conjunto de informes para la gestión del transporte y aplicación para la exportación de los datos de ventas sobre las aplicaciones propias de ALSA.

GMV llevará a cabo el suministro en los próximos meses, ya que entrará el sistema en producción antes de la finalización del año 2021.

GMV suministra su sistema de billetaje basado en la nube para el transporte público de Malta

Malta tiene en el turismo una de sus principales fuentes de ingresos y, por ello, su sistema tarifario debe ser de primer orden. Consciente de esta prioridad, CONCESIONES UNIFICADAS acudió a GMV para el despliegue en el transporte público de Malta del sistema de billetaje basado en la nube (ABT).

GMV opera desde hace seis años en Malta su sistema inteligente de transporte (ITS), desarrollado internamente, que incluye los sistemas integrados de ayuda a la explotación, billetaje (pago con tarjeta), información al pasajero y videovigilancia embarcada para una flota de más de 400 vehículos.

El ABT permitirá la rápida adaptación de los sistemas a las nuevas políticas tarifarias, así como la transferencia de normas entre distintos medios de transporte desde una misma central administrativa, sin que afecte ningún cambio a los equipos embarcados.

El sistema ABT es fácil de mantener; la parte lógica de las tarifas se gestiona y procesa de manera centralizada en la unidad administrativa y no en los equipos embarcados, lo que significa que el sistema se puede actualizar rápidamente y adaptarse con facilidad a los avances tecnológicos. En comparación con este sistema ABT de bajo mantenimiento, que trabaja con una única central administrativa, resulta extremadamente alto el mantenimiento que se requiere para toda una red de equipos albergados localmente.

El título de transporte tradicional es sustituido en el sistema ABT por un token de identificación.

GMV podrá incorporar este sistema ABT a los equipos instalados en la actualidad. Este proyecto incluye el software de adaptación del sistema de billetaje general para los equipos embarcados y para la central de administración. El programa piloto se pondrá en marcha en seis meses y, una vez finalizado, el actual sistema basado en la tradicional tarjeta migrará al sistema ABT, sin que sea necesario sustituir la tarjeta de transporte ya existente, que podrá utilizarse como token de identificación.

GMV renueva los contratos de mantenimiento de SAE y de SIP de Polonia

A finales de 2020, GMV firmó su tercer contrato consecutivo de servicio posgarantía para los sistemas de ITS de Szczecin. En virtud de este acuerdo, en 2021 GMV realizará el mantenimiento del sistema de gestión de flotas (SAE) y el de información a los pasajeros (SIP) dentro del ámbito del software central, las unidades de a bordo de 437 vehículos y 93 paneles LED en las paradas.

El contrato también incluye el sistema completo de emisión de billetes electrónicos con el software central, 36 máquinas expendedoras de billetes fijas que admiten pagos en efectivo y de comunicación de campo cercano (NFC) y según la norma EMV sin efectivo, 317 máquinas móviles expendedoras de billetes que admiten pagos en efectivo, NFC y EMV sin efectivo, así como 1679 validadores NFC a bordo. También quedan cubiertos por GMV otros subsistemas como el sistema de videovigilancia de circuito cerrado de televisión (CCTV) de a bordo o el sistema de recuento automático de pasajeros.

Mediante un acuerdo suscrito con Tranvías de Varsovia, en 2021 GMV se encargará del mantenimiento de los geolocalizadores de a bordo de 530 tranvías, así como del envío de los datos de posicionamiento por GPS de los vehículos a los centros de control del cliente.

Además, este mismo año GMV proporcionará a la autoridad municipal de carreteras y transporte público de Bydgoszcz los servicios de conservación y mantenimiento de los servidores junto con el software central del SAE, 125 paneles LCD en las paradas y unidades GPS a bordo de 325 autobuses y tranvías de transporte público.

Desde 2021, GMV prestará en Toruń la asistencia técnica integral para todos los elementos del sistema central de gestión de flotas y de información dinámica para los pasajeros, incluido el software de la central del SAE, las unidades de a bordo de 51 tranvías y 67 paneles LED de las paradas.

Puesta en operación de nuevos sistemas CCTV en series de trenes de Metro de Barcelona

GMV ha completado exitosamente la implantación del sistema de videovigilancia embarcada en los 47 trenes de las series 5000 y 6000 de Metro de Barcelona, así como en los 10 trenes de las nuevas series 5000 y 6000 que suministra CAF a TMB.

Dentro del alcance del proyecto, por cada tren se ha desplegado una red Ethernet embarcada multiservicio en anillo con un *switch* por coche que soporta no sólo el nuevo sistema de video vigilancia, sino también el transporte de otros sistemas a futuro.

Se ha suministrado como grabador digital de vídeo (NVR) un equipo de diseño propio de GMV, que es capaz de realizar la grabación de imágenes en formato Full HD y la reproducción y exportación de forma simultánea de estos vídeos. Se han instalado dos NVR por tren que trabajan en modo redundante. En caso de *failover*, el NVR activo asumirá la grabación de todas las cámaras de manera automática y autónoma.

El sistema cuenta con nodos concentradores de comunicaciones que son responsables de gestionar la información embarcada, ya sea proveniente del sistema de video vigilancia u otros, así como de ponerla a disposición de tierra a través de los canales de comunicaciones inalámbricos más apropiados en función de la ubicación del tren y las coberturas disponibles. Se dispone para ello de conectividad WIFI y 4G/LTE.

La solución se ha completado con cámaras IP y cámaras IP con infrarrojos para cabina en los nuevos trenes de CAF y con codificadores analógico-digitales que han permitido la reutilización de las cámaras analógicas existentes en algunos trenes.

Asimismo, se ha puesto en marcha en tierra un servidor de videovigilancia centralizado así como puestos de operador en los centros de control de metro y de seguridad, así como en protección civil de la base de Sagrera.

Finaliza el proyecto Urban Air para la movilidad sostenible en Valladolid

El proyecto Urban Air es parte de las iniciativas del Programa Interreg para la cooperación transfronteriza entre España y Portugal. Liderado por la Universidad de Valladolid, el proyecto busca desarrollar propuestas de movilidad con especial énfasis en la movilidad mediante el uso compartido de bicicletas. Con el objetivo de cuantificar la reducción en la huella de carbono asociada al despliegue de este sistema, se han integrado en las bicicletas una serie de sensores que miden la calidad del aire a lo largo de los trayectos de los usuarios.

En el marco del proyecto, GMV ha desarrollado una aplicación móvil que gestiona el uso compartido de las bicicletas mediante candados inteligentes que se comunican a través de Bluetooth® para permitir a los usuarios el acceso a las mismas. La aplicación permite monitorizar los viajes realizados por los usuarios y conectar el teléfono con los sensores integrados. De este modo, los usuarios pueden conocer la calidad del aire a lo largo de su recorrido habitual y cuantificar el ahorro de emisiones que supone el desplazamiento en bicicleta en lugar del vehículo privado.

La situación de la pandemia ha condicionado el proyecto, debido a que no es posible garantizar la desinfección de las bicicletas entre los usuarios. Así, durante estos meses, se ha tenido que transformar el sistema de uso compartido de bicicletas a un sistema de préstamo en el que a cada usuario se le asigna el uso de la bicicleta por un período de tiempo determinado.

En este sentido, GMV ha adaptado el sistema de préstamo de bicicletas para que funcione mediante la asignación única de vehículos a usuarios. En la actualidad, el servicio de préstamo de bicicletas está operativo en la Universidad de Valladolid con 50 bicicletas operativas y ya se está gestionando el préstamo de bicicletas para el próximo curso lectivo.

Urban Air

Interreg
España - Portugal

Curso sobre ITS para el pago por uso de las carreteras

GMV participó a principios de marzo en un evento en formato mixto *online*/ presencial bajo el título «Curso sobre ITS para el pago por uso de las carreteras», organizado por ITS España y coordinado por ARUP.

En representación de la compañía, Carlos Barredo, jefe de la división de Aftermarket y R&D en el área de automoción de GMV, habló sobre los sistemas basados en tecnologías satelitales en los que la compañía trabaja. Durante su intervención, definió el concepto y la arquitectura de estos sistemas, con sus diferentes elementos que incluyen plataforma de *backoffice*, sistema de comunicaciones, subsistema de control o *enforcement* y la unidad embarcada (OBU).

Además, Barredo explicó todos los conocimientos y las soluciones de GMV en sistemas de pago por el uso de la infraestructura basados en tecnología GNSS. En particular, aquellos aspectos relacionados con el uso del *smartphone* como plataforma de usuario y tecnología de cobro, con la posibilidad de ampliar este tipo de arquitectura a la gestión de las zonas de bajas emisiones en las ciudades.

También expuso la experiencia de GMV en este ámbito a través de distintos casos de éxito, así como las sinergias existentes con los servicios C-ITS y otros servicios conectados en el vehículo.

Finaliza TachograAPP, el estudio de la CE para un transporte seguro

GMV ha realizado un estudio con un recopilatorio de posibles soluciones que integren tecnologías de comunicaciones y posicionamiento de satélites con el fin de poder identificar cómo aplicarlas en la monitorización de vehículos de transporte de pasajeros y mercancías

El estudio TachograAPP, financiado por la Dirección General de Movilidad y Transporte en Europa (DG-MOVE), coordinado por VVA y liderado por GMV en el análisis técnico, ha finalizado. El objetivo de este estudio ha sido el análisis y estudio de la posibilidad de aplicar las tecnologías desarrolladas en el ámbito de la telefonía móvil para definir las posibles evoluciones del tacógrafo inteligente.

Según la regulación vigente desde junio de 2019, todos los vehículos de más de 3,5 toneladas de peso para transporte de mercancías o de más de 9 personas deben estar equipados con un tacógrafo inteligente. Este dispositivo registra la actividad del vehículo para asegurar que se cumple la normativa respecto a tiempos de trabajo y descanso de los conductores con el objetivo de minimizar los accidentes en carretera debidos al exceso de fatiga.

Sin embargo, son muchos los casos de fraude detectados por las autoridades durante los controles rutinarios, ya que existe un claro beneficio económico en ignorar los tiempos de descanso para realizar más portes, a pesar del riesgo que supone para el conductor y los demás usuarios de la vía pública.

Para mejorar la seguridad de todos, así como reducir el fraude y combatir las mafias que se dedican a modificar y deshabilitar los tacógrafos actuales, la Comisión Europea investiga nuevas soluciones que integren los últimos avances disponibles en tecnología de comunicaciones, sensores, posicionamiento por satélite, autenticación biométrica y seguridad informática.

El estudio, realizado por GMV, ofrece a la DG-MOVE un recopilatorio de posibles soluciones que integren estas tecnologías con el fin de poder identificar cómo aplicarlas en la monitorización de vehículos de transporte de pasajeros y mercancías. De este modo, es posible mejorar el control sobre la actividad de los vehículos, así como preservar o mejorar el nivel de seguridad ofrecido por la solución actual (EAL 4+).

Como conclusión del análisis realizado, se ha verificado la viabilidad de la combinación de estas tecnologías en el vehículo, así como el análisis de datos en la nube. Esto permitiría a las autoridades de tráfico detectar las infracciones en tiempo real, comunicarse remotamente e intercambiar información con los vehículos que reporten condiciones inusuales.

Además, reduciría la carga de trabajo de los agentes encargados de los controles en carretera y contribuiría a poder verificar las condiciones de conducción de un mayor número de vehículos simultáneamente. Gracias a estos factores se reduciría el fraude en la carretera y la posibilidad de accidentes asociados al exceso de fatiga de los conductores.

GMV continúa apostando por impulsar la ciberseguridad en el vehículo

La ciberseguridad de los vehículos conectados y autónomos es una de las principales fuentes de debate en la comunidad de automoción, especialmente frente a las nuevas regulaciones de ciberseguridad como UNECE WP.29 e ISO-21434.

Desde hace años, GMV trabaja en nuevas técnicas de protección de seguridad para las comunicaciones de los vehículos y desarrolla su actividad en escenarios en constante evolución.

Con el fin de responder a las nuevas amenazas y desafíos, GMV impulsa su proyecto de ciberseguridad aplicada a la automoción, evolucionando su modelo de IDPS para vehículo conectado y autónomo y explorando nuevas soluciones para hacer la conectividad V2X más robusta.

Uno de los principales objetivos de GMV para 2021 es el despliegue de un sistema de detección de intrusiones en el vehículo basado en algoritmos de inteligencia artificial en tiempo real (AI-IDS).

El proyecto tiene como alcance principal la evolución de nuestro AI-IDS, capaz de proporcionar un sistema determinista y basado en reglas, altamente configurable, que incorpore tecnologías de aprendizaje profundo para controlar el acceso y la autenticación en todas las comunicaciones e interfaces de un vehículo. Asimismo, el proyecto incorpora un componente que amplía el alcance a las comunicaciones entre vehículos e infraestructuras (V2X).

La infraestructura de clave pública vehicular (VPKI) se está imponiendo como solución de gestión de credenciales en las comunicaciones V2X. En el marco del proyecto, se plantea realizar un estudio para identificar todas las limitaciones y debilidades de los VPKI en términos de escalabilidad e interoperabilidad al tiempo que se propongan nuevas soluciones de gestión de credenciales para comunicaciones V2X.

El objetivo es mejorar la seguridad en tiempo de ejecución, la privacidad y la confiabilidad de los dispositivos con una solución escalable y descentralizada que elimine la necesidad de una infraestructura compleja como la estructura PKI.

En base a los primeros resultados, se considera que la aportación de GMV en todas estas nuevas arquitecturas puede ser parte del futuro de la ciberseguridad en el vehículo conectado y autónomo, y apreciado por sus clientes, tanto OEMs como suministradores TIER Is.

GMV participa en el *webinar* del piloto de Madrid desplegado en el proyecto C-ROADS

GMV participó el 4 de febrero en el *webinar* del piloto de Madrid desplegado en el proyecto C-ROADS, organizado por ITS España. En el *webinar* se presentaron los principales datos del despliegue y se trataron los aspectos más relevantes que se están abordando gracias a la participación de las entidades involucradas.

GMV es proveedor de las OBUs (*On-Board Units*) y además pone a disposición de la entidad que hace el análisis de datos una página web donde se muestran *logs* tanto de las OBUs como del HMI. También se registran otros tipos de datos como los mensajes recibidos en las OBUs desde las RSUs (*Road Side Units*) y logs de navegación.

GMV presentó los equipos embarcados en los vehículos y el rol que toman dentro de la arquitectura de sistemas cooperativos C-ITS, basados en comunicaciones V2X. Se explicó la interacción de estas piezas claves del despliegue de sistemas C-ITS con el resto de elementos de la red viaria, así como el papel que toman el HMI y el servidor de GMV, el cual recibe información de fuentes como la plataforma DGT3.0 y MC30.

Además, se mostraron varios ejemplos de la interfaz de usuario de la aplicación de *smartphone* para diversos casos de uso de los servicios Día 1, Día 1.5 y servicios de comunicaciones híbridas, con el objetivo de mejorar la conducción y seguridad vial del conductor y su entorno.

Por último, se mostró la web de gestión de vehículos y la web de registro de datos desplegada por GMV explicando sus diversas funcionalidades.

GMV colabora en las certificaciones de los casos de uso en la plataforma DGT 3.0

La plataforma del vehículo conectado DGT 3.0 es una iniciativa de la Dirección General de Tráfico que facilita el intercambio de datos en tiempo real de todos los actores implicados en la movilidad para alcanzar el objetivo de Visión Cero: 0 fallecidos, 0 lesionados, 0 congestión y 0 emisiones.

GMV apuesta por los sistemas cooperativos y por esta base para conseguir una movilidad más inteligente, sostenible y segura, que reducirá el riesgo de accidentes en toda la red de carreteras de España.

Dentro del proyecto europeo C-ROADS, GMV ha desarrollado una aplicación de *smartphone* que además de servir de HMI (interfaz hombre-máquina, por sus siglas en inglés) para la OBU (*On-Board Units*) embarcada en el vehículo, permite dentro del piloto DGT3.0 informar a los usuarios sobre cualquier evento próximo durante su trayecto para una mejor toma de decisiones en la conducción. La aplicación ha sido desarrollada tanto para entorno iOS como Android.

A finales de 2020 se realizó con éxito la integración con la plataforma DGT 3.0 en relación con los casos de uso de obras planificadas e incidencias. En la certificación del caso de uso de obras planificadas, se comprobó cómo la aplicación en el *smartphone* recibía la información de la plataforma DGT 3.0 y notificaba al usuario sobre la existencia de una obra próxima. El conductor cambiaba de carril con anterioridad y reducía previamente su velocidad con suavidad para evitar cambios bruscos al volante.

Por otro lado, en la certificación del caso de uso de incidencias, se verificó la recepción de información desde el Centro de Gestión de Tráfico de la DGT sobre un vehículo detenido en la vía y se demostró cómo el usuario podía anticipar su reacción ante este evento.

Los casos de uso de obras planificadas e incidencias se suman a la lista de los casos de uso ya desplegados e integrados anteriormente de mensaje virtual (PMV) y señal V-16.

Desde GMV se continuará con la integración con la plataforma de vehículos conectados DGT 3.0 a medida que nuevos servicios se hagan disponibles, además de seguir apostando por estas iniciativas tecnológicas avanzadas que permiten una mejora de la seguridad y la movilidad sostenible.

GMV desarrolla la nueva web de EUMETSAT

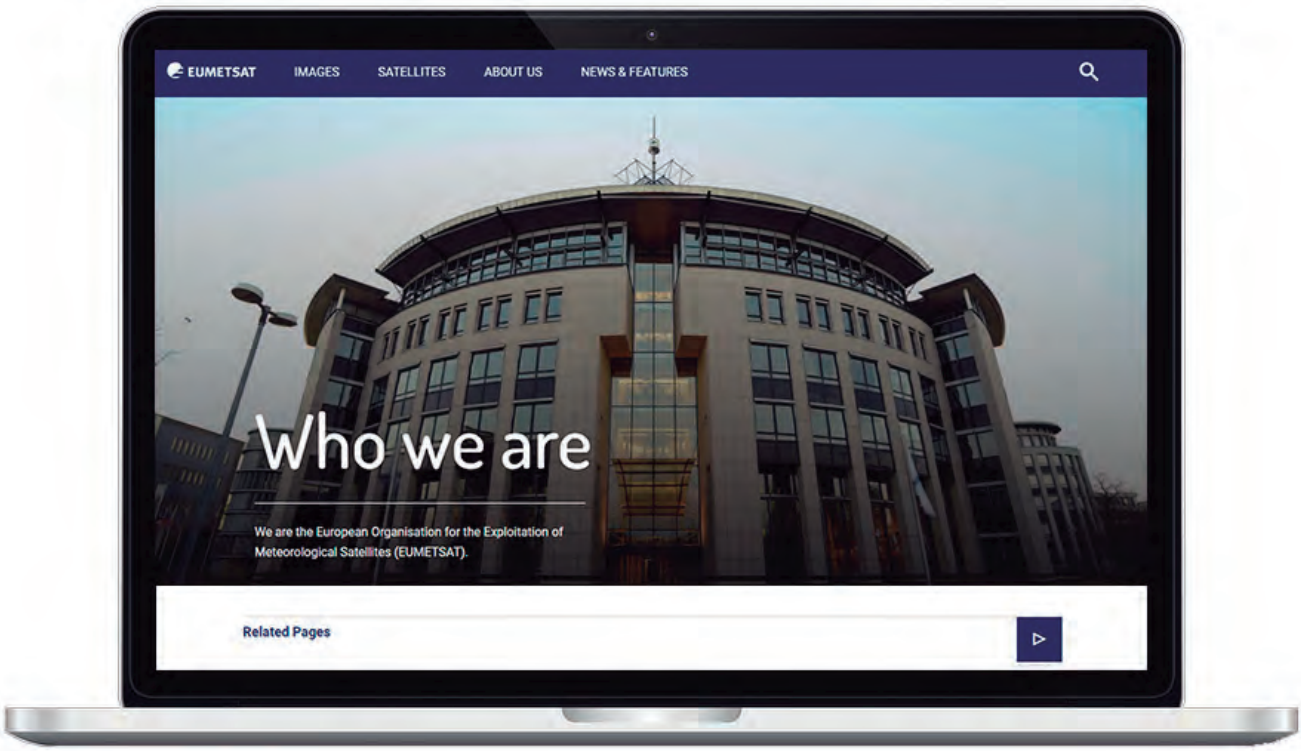
EUMETSAT, la Organización Europea de Satélites Meteorológicos, ha renovado con la colaboración de GMV su sitio web, utilizando las últimas tendencias en desarrollo y los servicios más avanzados de ciberseguridad.

Como resultado de la madurez en todos los campos tecnológicos requeridos para llevar a cabo el proyecto (desarrollo web, *hosting*, ingeniería, servicios gestionados y respuesta a incidentes), GMV ha proporcionado una solución más integrada, más fácil de gestionar y con los más altos estándares de calidad. Además, tras más de diez años de colaboración en diferentes actividades y unidades de EUMETSAT, GMV posee un profundo conocimiento de la organización, sus procedimientos e infraestructura.

La nueva web desarrollada y puesta en producción evoluciona la antigua arquitectura del portal web hacia un gestor de contenidos de última generación. Alojado completamente en la nube de Amazon Web Services (AWS), se beneficia así de todas las capacidades de una plataforma auto escalable y altamente fiable, reduciendo los costes de operación y mantenimiento y minimizando los períodos de indisponibilidad por tareas de actualización o mantenimiento.

Esta nueva plataforma utiliza la red de entrega de contenido de AWS (*CloudFront*) para mejorar el rendimiento, haciendo que los tiempos de respuesta sean muy bajos.

En definitiva, con respecto a la versión anterior, la nueva web ofrece mejoras en continuidad, contingencia, escalabilidad y flexibilidad. Uno de los aspectos fundamentales del proyecto es la provisión de los servicios de ciberseguridad. En este sentido, el nuevo sitio web está monitorizado por el Equipo de Respuesta ante Emergencias Informáticas, GMV-CERT. De esta forma se consigue el nivel de ciberseguridad requerido en este tipo de instalaciones.



Opinión

Cloud Computing en tiempos de pandemia

La adopción del *cloud* en España sigue subiendo de forma clara y sin pausa. Según IDC Research España, en el informe «Soluciones Multi*cloud* para la Transformación Digital», en 2022 el 40 % del gasto principal de TI estará relacionado con la nube. Cada vez son más las empresas que tienden hacia este modelo, transportando parte de sus sistemas (inicialmente los menos críticos) para más adelante ampliar el alcance con servicios cada vez más críticos.

En Europa se están empezando a mover iniciativas como la «EU Federations of *Cloud*» o «GAIA-X». En este sentido, España no está mal posicionada y las perspectivas son de crecimiento con algo más de presencia en territorio nacional de infraestructura propia de los grandes proveedores de *cloud*.

Efectos de la situación COVID-19 en la *Cloud*

Esta crisis ha supuesto una serie de cambios y nuevas condiciones que han acelerado todavía más la adopción del modelo *cloud*, principalmente por la flexibilidad y autonomía que supone su utilización. De la misma forma que los ataques del 11-S hace casi dos décadas pusieron el foco en los centros de respaldo y los planes de contingencia, ahora la pandemia causada por la COVID-19 ha provocado una mayor importancia de la flexibilización y capacidad de dispersión de los sistemas, principalmente por el teletrabajo y limitaciones a la movilidad.

Las dudas en cuanto a la seguridad de la nube pública siguen existiendo, especialmente en lo referente a la confidencialidad de mis datos. ¿Quién puede acceder a mis datos? ¿Hay puertas traseras? ¿Se pueden enviar mis datos a determinados países? Por este motivo es importante asegurarse que implementamos las medidas de seguridad adecuadas a nuestros sistemas: CASB, cifrado de datos, DLP, IAM, etc.

Presente y futuro de los modelos *cloud*

Dentro del proceso de transformación digital que están abordando muchas empresas el modelo *cloud* más indicado, en general, es el modelo híbrido, donde los activos más importantes estarían en el *datacenter on premise* y el resto podrían estar en la nube pública.

La principal ventaja que aporta este modelo es tener recursos rápidamente en la nube pública tanto para cubrir picos como para nuevas necesidades, sin depender en exclusiva de la nube pública. Además, podemos conseguir unos porcentajes muy altos de aprovechamiento de la infraestructura *on premise*, al no ser necesario un dimensionamiento para picos. Desde el punto de vista de la seguridad, supone una ventaja importante ya que reducimos mucho los riesgos, siempre que se controle adecuadamente qué datos y qué sistemas desplegamos en la parte *on premise* y cuales en la nube pública.

La tendencia es ir hacia soluciones *multi-cloud* que permiten desplegar en varias nubes, pudiendo mover el contenido entre ellas para mejorar el servicio, optimizar costes o minimizar riesgos. Es fundamental que el diseño sea agnóstico del *cloud*, no dependiendo de servicios específicos de un proveedor *cloud*, que nos pueda impedir en un futuro salir de esa nube o mover contenidos entre diferentes nubes públicas. Hay que tener en cuenta que podemos tener penalizaciones económicas por mover datos a otras nubes públicas. De ahí la importancia de un diseño y asesoramiento adecuado.

Antonio Cabañas
Director de la división Ciberseguridad e Infraestructuras de Secure e-Solutions de GMV

Esta crisis ha supuesto una serie de cambios y nuevas condiciones que han acelerado todavía más la adopción del modelo *cloud*, principalmente por la flexibilidad y autonomía que supone su utilización

GMV colabora en la IX Guía de referencia Smart Energy de enerTIC

Un año más, GMV ha colaborado en la IX Guía de Referencia Smart Energy «Tecnología para la mejora de la Eficiencia Energética». Bajo el título «Buenas prácticas, soluciones, 100 proveedores fundamentales y tendencias 2020», la guía, elaborada por la Plataforma enerTIC, ofrece una amplia perspectiva del potencial de transformación de la tecnología en el ámbito de la eficiencia energética y la sostenibilidad.

Esta edición profundiza sobre el impacto del gran fenómeno de la transformación digital, incidiendo en la mejora de competitividad y sostenibilidad a través las nuevas tendencias tecnológicas con la vista puesta en la consecución de los objetivos de desarrollo sostenible (ODS) para el año 2030.

En la guía se recogen las tendencias para el 2021 por parte de los grupos de expertos de la plataforma enerTIC. Miguel Hormigo, director sector Industria de Secure e-Solutions de GMV, destaca los sistemas inmersivos para cambiar los sistemas tradicionales del teletrabajo, la mejora en las telecomunicaciones para aumentar la calidad y la experiencia de usuario, la sensorización inteligente para la toma de decisiones basada en IoT y la hiperautomatización, es decir, la búsqueda de la automatización inteligente (robótica e IA) de cualquier proceso productivo susceptible de mejorar en busca de la disminución de la presencia física en los entornos de trabajo.

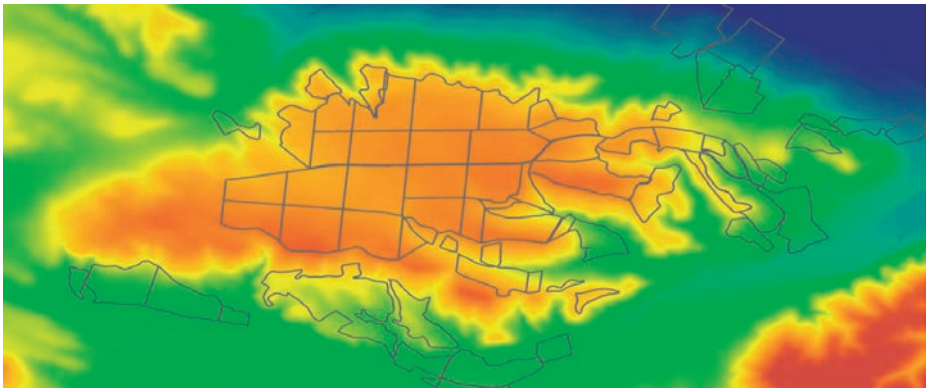
Un documento clave para que los directivos que lideran las estrategias de tecnología, innovación, operaciones y sostenibilidad puedan conocer los últimos avances y las soluciones tecnológicas de mayor impacto para la competitividad y la eficiencia.

Innovación y digitalización, aspectos esenciales del desarrollo de la agricultura

La innovación, la digitalización y la sostenibilidad son objetivos y herramientas indispensables para el futuro del sector agrario. Tenemos que ser capaces de cambiar las formas de producir, utilizar las herramientas tecnológicas y aprovechar todos los datos del entorno para poder trabajar con inteligencia en el campo.

Durante la tercera jornada de AgroExpo, evento organizado por la Institución Ferial de Extremadura (FEVAL) y punto de encuentro para el sector agrario, GMV centró su ponencia en la innovación y la integración de las tecnologías como uno de los pilares de la agricultura inteligente.

En primer lugar, Miguel Hormigo, director del sector Industria, mostró las soluciones y tecnologías aplicadas a Smart Agro en las que GMV está trabajando: inteligencia artificial para clasificar imágenes, mantenimiento operacional y predictivo, desarrollo de sensores e integración de redes IoT para la trazabilidad y necesidades específicas, automatización de procesos y robótica, etc.



A continuación, Antonio Tabasco, responsable del área de Teledetección y Análisis geoespacial de GMV, explicó con más detalle ***Wineo***, el servicio avanzado de análisis de datos geoespaciales que apoya la toma de decisiones en agricultura. La solución ***Wineo*** procesa e integra todos los datos de múltiples fuentes (datos agroclimáticos, imágenes de satélite y sensórica IoT) por medio de una estrategia de aprendizaje automático de modelización de cultivos basada en un análisis avanzado de datos. Esto permite proporcionar una capa inteligente al análisis de campo para apoyar el diseño de campañas de fertilización, monitorización del crecimiento, recomendaciones de riego y estimaciones precisas de rendimiento y como apoyo a la toma de decisiones en base a datos objetivos.

GMV abre una oficina permanente en Bruselas

La oficina trabajará en estrecha cooperación con las instituciones de la UE, en particular con la Comisión Europea, el Consejo de la Unión Europea, el Parlamento Europeo y las Agencias de la UE

GMV, con una fuerte presencia en la UE y empresas establecidas en siete Estados miembro, es ya el sexto grupo industrial que más empleo genera en el sector espacial en Europa. En consonancia con esta tendencia de crecimiento, la empresa ha creado una oficina permanente en Bruselas con el fin de reforzar el diálogo con la UE y promover una comunicación continua y constructiva con las diversas instituciones y partes interesadas. De este modo, contribuirá a la configuración y la ejecución de la agenda de la UE y abordará además los importantes retos y oportunidades de las principales áreas de actividad de la compañía: espacio, defensa, tecnologías de la información y comunicaciones y transporte.

La oficina de GMV en Bruselas trabajará en estrecha cooperación con las instituciones de la UE, en particular con la Comisión Europea, el Consejo de la Unión Europea, el Parlamento Europeo y las Agencias de la UE. La nueva oficina servirá también de enlace con las Representaciones Permanentes nacionales ante la UE, así como con el Comité de Representantes Permanentes con el propósito de incorporar las opiniones de los representantes de empresas y del sector al proceso de toma de decisiones. Asimismo, trabajará a nivel local junto con socios y asociaciones industriales y con las administraciones públicas en la búsqueda de la mejor manera de contribuir al crecimiento de los sectores en los que opera la empresa.

GMV contribuye de manera clave en programas emblemáticos de la UE, como Galileo, Copernicus, SST, Govsatcom y Horizon Europe, en los que desempeña una función primordial en la ejecución de las agendas de seguridad y defensa, particularmente en lo tocante a los Fondos de Defensa Europeos. Desde su oficina de Bruselas, la empresa proporcionará presencia local para reforzar la comunicación y la coordinación en el marco de los programas de la EU actualmente en marcha y en las nuevas iniciativas, como *Secure Connectivity Constellation, Quantum Encrypted Communications* y *Space Traffic Management*.

La oficina, situada en pleno corazón del Barrio Europeo de Bruselas, será también lugar de encuentro e intercambio de ideas sobre las políticas industriales y los programas de la UE.

GMV dona 50.000 euros al Banco Mundial de Alimentos

La situación generada por la COVID-19 ha hecho que los habituales eventos presenciales con empleados se celebren en formato *online* y que las acciones previstas tengan además un cariz solidario. Tal fue el caso del tradicional evento navideño organizado por GMV en modalidad telemática y que culminó con un brindis solidario.

Conscientes de que una de las consecuencias provocadas por esta pandemia está siendo la crisis económica y la carestía alimentaria, los empleados de GMV decidieron donar al Banco Mundial de Alimentos el importe del regalo previsto para el brindis, a través de la acción «un brindis solidario». Esta respuesta solidaria por parte de los empleados alcanzó un total de 35.860 €, importe que ha sido completado hasta 50.000 € como aportación extra de la empresa a la institución.

El Banco Mundial de Alimentos es una de las organizaciones humanitarias que en estos tiempos está redoblando sus esfuerzos ante el aluvión de peticiones de alimentos y artículos de primera necesidad para hacer frente a la crisis sanitaria, económica y social como consecuencia de la COVID-19.

Con este gesto solidario por parte de GMV se pone de manifiesto la trascendencia que tienen hoy en día la cultura y los valores corporativos de la compañía. Unos valores entre los que destacan la generosidad, la solidaridad, la cooperación o el compromiso y que han trascendido en el apoyo a la labor humanitaria que el Banco Mundial de Alimentos está realizando. En este mismo contexto, tanto GMV como sus empleados a título personal, han participado durante los últimos meses en distintas acciones solidarias destinadas a paliar esta crisis.

La donación fue entregada el día 10 de marzo por Ignacio Ramos Gorostiola, director corporativo de People Strategy & Infrastructures de GMV en nombre de sus empleados y la empresa.

Ciencia y Tecnología en Femenino

Con motivo del Día Internacional de la Mujer y la Niña en la Ciencia, el 11 de febrero GMV celebró el *webinar* «Ciencia y Tecnología en Femenino» con el objetivo de poner de relieve el papel de la mujer en el ámbito de la ciencia y la tecnología y destacar la importancia de incentivar las vocaciones científico tecnológicas entre las jóvenes.

El encuentro contó con la participación de Silvia Abarca, ingeniera de proyectos de Espacio de GMV; Ana Sastre, desarrolladora de software de Defensa de GMV; Paloma Trigueros, responsable de Servicios Digitales de Sanidad de Secure e-Solutions de GMV, y Cristina Muñoz, ingeniera de proyectos para Automoción de Sistemas Inteligentes de Transporte de GMV.

Durante la mesa redonda, las ponentes señalaron algunos de los factores que más están incidiendo en este contexto de desigualdad y que, por tanto, pueden ejercer de motores de cambio. Entre ellos destacaron el factor cultural, los planes educativos o los medios de comunicación.

La igualdad de género en las aulas se traduce en igualdad de oportunidades en el ámbito laboral y esto desemboca en una sociedad más equilibrada. El objetivo no es la feminización, sino lograr el equilibrio entre hombres y mujeres. Por eso, es necesario intensificar medidas como la divulgación científica de la mano de mujeres, la visibilidad de referentes femeninos en los medios de comunicación, el empoderamiento de las jóvenes estudiantes a través de iniciativas de orientación y la concienciación de la sociedad para cambiar los estereotipos porque el talento no entiende de género.

GMV fomenta la vocación tecnológica y el talento STEM

Consciente del reto que plantea la necesidad de promover la investigación científica y tecnológica en disciplinas STEM, GMV lleva más de una década participando en distintas iniciativas dedicadas a fomentar la vocación estudiantil hacía estas disciplinas

Hace más de una década que desde las empresas se mira a las universidades y centros de enseñanza en busca de futuros profesionales STEM que cubran la creciente demanda laboral. Sin embargo las carreras de ciencia, tecnología, ingeniería o matemáticas, o más conocidas como STEM, no solo no consiguen reunir estudiantes en sus diferentes ramas, sino que los van perdiendo curso tras curso. Una situación que se traslada directamente al mercado laboral y de ahí a las empresas, que encuentran serias dificultades para captar y fidelizar talento.

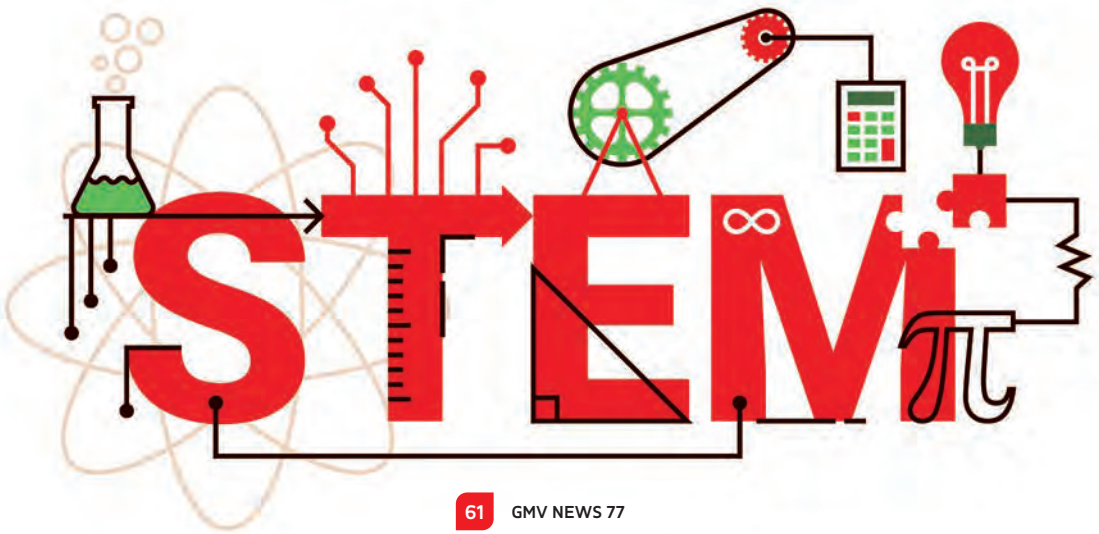
Esta situación se acentúa en el caso de las mujeres, que tradicionalmente han sido minoría en las carreras tecnológicas. Dentro de los estudios STEM, las mujeres siguen siendo una minoría, ya sea por barreras culturales, estereotipos o por una ausencia de referentes en los que inspirarse. Según el estudio de la Unesco «Descifrar el código» solo el 35 % de los estudiantes matriculados en STEM en todo el mundo son mujeres. Mientras que en el ámbito de los equipos de investigación, la presencia femenina alcanza únicamente el 28 %.

Hacer frente a algunos de los mayores desafíos de la Agenda para el Desarrollo Sostenible —desde la mejora de la salud hasta el cambio climático— dependerá del aprovechamiento de todo el talento. Eso significa atraer tanto a hombres como a mujeres hacia estas disciplinas. La diversidad en la investigación amplía el número de talento y aporta nuevas perspectivas, capacidades y creatividad.

Tanto gobiernos como empresas ya no dudan de la necesidad de promover la investigación científica y tecnológica, así como animar a los jóvenes a acercarse a las carreras STEM. Se trata de impulsar la formación basada en la investigación, de difundir el impacto de la ciencia en la sociedad, de fomentar el uso de las TIC en las aulas y de que se empleen nuevos recursos educativos.

Teniendo muy presente sus raíces, GMV colabora en diferentes eventos y organiza distintas iniciativas en el marco académico con el objetivo de fomentar la pasión por el mundo tecnológico. Consciente, además, del reto que plantea la necesidad de promover la investigación científica y tecnológica en disciplinas STEM, GMV lleva más de una década participando en varias iniciativas dedicadas a fomentar la vocación estudiantil hacía esas disciplinas, incidiendo en aquellas orientadas en aumentar el atractivo de la educación científica y las carreras científicas entre las mujeres.

Para esta labor, GMV cuenta con el apoyo de algunas mentoras con perfiles científico-tecnológicos que dedican parte de su tiempo a compartir la pasión de trabajar en profesiones STEM. En este artículo dos de estas mujeres comparten su experiencia y nos ofrecen su punto de vista sobre la importancia de promocionar estas vocaciones.



Mariella Graziano

Executive Director of Strategy and Business Development/Flight Systems and Robotics. Espacio

Muchas veces me han preguntado y me he preguntado por qué he elegido estudiar ingeniería y la realidad es que no tengo una respuesta. El cuándo lo tengo claro. Desde muy pequeña mi intención era ser médico. Viajé a Roma para apuntarme a la facultad de Medicina y volví apuntada a la de Ingeniería. Gran disgusto de mi familia que así perdía una generación de médicos, tradición familiar.

La verdad es que no soy una ingeniera de manual, e ingeniera espacial aún menos. Nunca me ha gustado la ciencia ficción, no he visto ninguna película de Star Wars o puede que una si la haya visto. En mi carrera todo ha sido un poco casualidad. Vengo de un pueblo pequeñísimo en el medio de las montañas donde lo que gana es la libertad y el contacto con la naturaleza.

Creo que soy ingeniera porque siempre he querido saber cómo funcionaban las cosas. Mis abuelas, gente humilde y analfabeta aunque mis primeras maestras y referentes, me han enseñado mucho dándome sus explicaciones de gente de campo. La ingeniería me ha demostrado que lo que me decían era cierto, aunque las explicaciones eran a veces bastante más complejas. No hay mucha diferencia en por qué vuela un halcón o un avión. Para mi es igual de atractivo aterrizar en la luna que ver cómo sube la masa de una buena pizza. Lo que hace la diferencia es saber quién eres y por qué te mueves. Esto es lo que intento trasmitir cuando hablo con los jóvenes talentos.

Participo en muchos programas de «STEAM» (añado la A de Arte porque para ser un buen ingeniero hace falta mucha creatividad a pesar de la fama de aburridos que tenemos), he dado charlas a jóvenes de todas las edades, desde la guardería hasta la universidad. Lo que siempre hago es contar mi experiencia. Creo que no hay nada más atractivo para alguien que se está formando y que está tomando decisiones que una experiencia real. Creo que nuestra sociedad pone una presión muy fuerte sobre todos, los jóvenes y las mujeres en particular. He escuchado a chicas decir que estaban en un concurso de robótica porque querían demostrar que las mujeres pueden hacer un robot. Siempre les he dicho que esto no va de demostrar nada a nadie. Esto va de hacer lo que te gusta de la mejor manera posible y con la mejor compañía al lado. Para esto hace falta primero saber lo que te gusta y luego mucho trabajo y algo de talento.

Aurora Izquierdo

Jefa de Sección. Sistemas Inteligentes de Transporte

Cuando GMV me animó a participar en el programa «Stem Talent Girl», hasta entonces desconocido para mí, no dudé en aceptar. Me entusiasmaba la idea de servir de referencia a chicas que se estén planteando una carrera científico-tecnológica como posibilidad de futuro. En mi caso, en ese sentido nunca tuve una referencia femenina próxima y, aunque yo siempre tuve clara mi vocación por las ciencias y la tecnología, esa falta de referencia probablemente haya truncado muchas potenciales ingenieras y científicas brillantes de varias generaciones.

Aunque aún queda mucho trabajo por hacer, también es cierto que con cada nueva generación las nuevas chicas STEM se van encontrando con más referentes de su mismo sexo, así como también con hombres concienciados de lo importante que es despertar la vocación científico-técnica en un 50 % de la población que históricamente no ha sido suficientemente motivada en ese camino. En este sentido, es esencial también que desde edades tempranas el profesorado sepa fomentar en el alumnado en general, tanto chicos como chicas, la curiosidad y la búsqueda del porqué, motores de la ciencia y de la ingeniería. En mi caso, tuve la suerte de recibir ese impulso en mi época de estudiante.

Por ello, a todas aquellas personas que estén considerando colaborar con en este tipo de iniciativas, les animaría a que lo hicieran. Es un trabajo tan necesario desde un punto de vista social, como gratificante a nivel personal. Y por otro lado, a las actuales estudiantes y futuras ingenieras y científicas, les animaría a que si tienen claro que esa es su vocación, vayan a por ello sin dudarlo. Se encontrarán un camino con menos obstáculos de los que encontraron sus predecesoras y en sus manos está seguir allanando el camino para nuestras sucesoras.

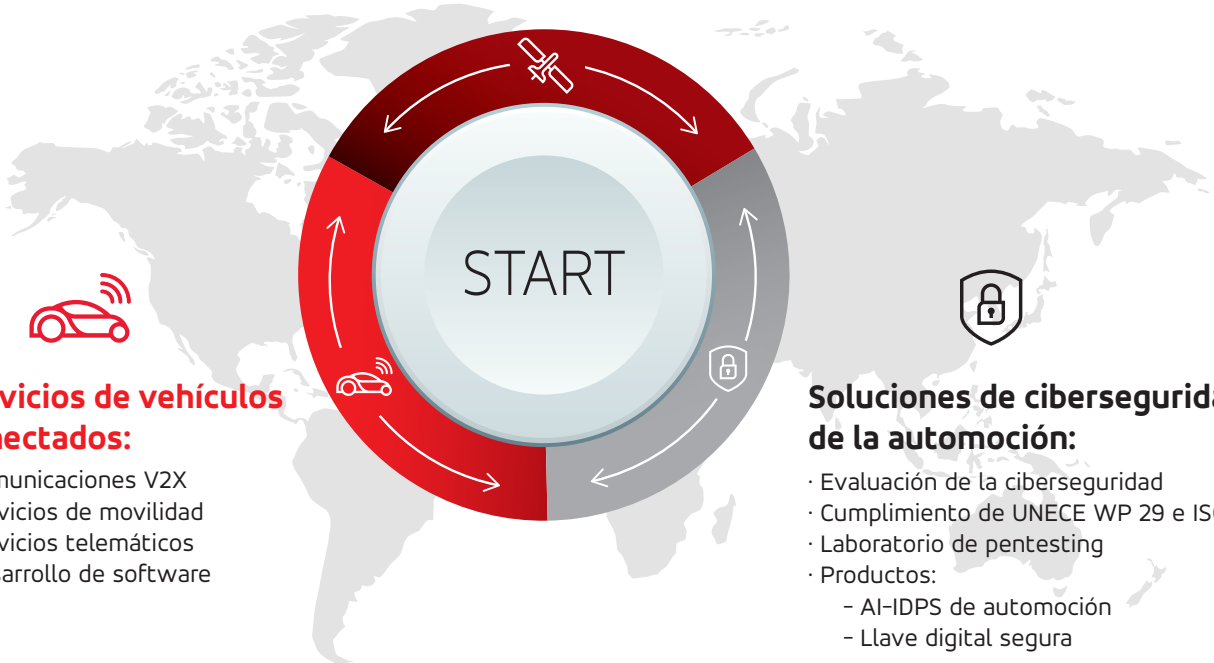
Tecnología GMV para automoción

La tecnología de GMV para automoción se basa en 3 ejes: los sistemas de posicionamiento para vehículo autónomo con tecnología GNSS; el área de ciberseguridad para automoción desarrollando servicios y productos específicos; y el área de vehículo conectado donde encontramos tecnologías relativas a las comunicaciones V2X, servicios de movilidad, servicios telemáticos y desarrollo de software seguro y fiable. Estos tres ejes son complementarios pudiendo integrarse entre sí.

gmv_aut@gmv.com

Suite de posicionamiento GNSS para conducción autónoma:

· Software embarcado de posicionamiento GNSS preciso y seguro
· Servicio de correcciones GNSS



Servicios de vehículos conectados:

· Comunicaciones V2X
· Servicios de movilidad
· Servicios telemáticos
· Desarrollo de software

Soluciones de ciberseguridad de la automoción:

· Evaluación de la ciberseguridad
· Cumplimiento de UNECE WP 29 e ISO 21434
· Laboratorio de pentesting
· Productos:
  - AI-IDPS de automoción
  - Llave digital segura

gmv®
INNOVATING SOLUTIONS

GMV en el mundo

ESPAÑA

OFICINAS CENTRALES

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

Santiago Grisolía, 4 P.T.M. Tres Cantos - 28760 Madrid
Tel.: 91 807 21 00 Fax: 91 807 21 99

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

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

Edificio Nova Gran Via, Avda. de la Granvia 16-20, 2ª planta
Hospitalet de Llobregat, 08902 Barcelona
Tel.: +34 932 721 848 Fax: +34 932 156 187

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

Edificio Sorolla Center, Nivel 1 Local 7, Av. Cortes Valencianas, 58 - 46015 Valencia
Tel.: +34 963 323 900 Fax: +34 963 323 901

Parque Empresarial Dinamiza. Avda. Ranillas, 1D - Edificio Dinamiza 1D, planta 3ª,
oficinas B y C - 50018 Zaragoza
Tel.: +34 976 50 68 08 Fax: +34 976 74 08 09

ALEMANIA

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

Capital Tower Bogotá, Calle 100 n.º 7-33, Torre 1, Planta 14- 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, 90014
Tel.: +1 (310) 728-6997 Fax: +1 (310) 734-6831

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.: (+603) 9205 8440 Fax: (+603) 9205 7788

POLONIA

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

PORTUGAL

Alameda dos Oceanos, 115, 1990-392 Lisboa
Tel.: +351 21 382 93 66 Fax: +351 21 386 64 93

REINO UNIDO

GMV NSL
HQ Building, Bldg 77. 1st floor. Thomson Avenue, Harwell Science and
Innovation Campus, Didcot,Oxfordshire OX11 0QG
Tel: +44 (0) 1865954477 Fax: +44 (0) 1865954473

GMV NSL
Sir Colin Campbell Building. Innovation Park. Triumph Road
Nottingham NG7 2TU
Tel: +44 (0) 1157486800 Fax: +44 (0) 1159682961

RUMANÍA

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